

# Optimality of Binning for Distributed Hypothesis Testing

Md. Saifur Rahman and Aaron B. Wagner<sup>\*</sup>

## Abstract

We study a hypothesis testing problem in which data is compressed distributively and sent to a detector that seeks to decide between two possible distributions for the data. The aim is to characterize all achievable encoding rates and exponents of the type 2 error probability when the type 1 error probability is at most a fixed value. For related problems in distributed source coding, schemes based on random binning perform well and often optimal. For distributed hypothesis testing, however, the use of binning is hindered by the fact that the overall error probability may be dominated by errors in binning process. We show that despite this complication, binning is optimal for a class of problems in which the goal is to “test against conditional independence.” We then use this optimality result to give an outer bound for a more general class of instances of the problem.

**Keywords:** distributed hypothesis testing, binning, test against conditional independence, Quantize-Bin-Test scheme, Gaussian many-help-one hypothesis testing against independence, Gel’fand and Pinsker hypothesis testing against independence, rate-exponent region, outer bound.

## 1 Introduction

Consider the problem of measuring the traffic on two links in a communication network and inferring whether the two links are carrying any common traffic [1, 2]. Evidently, this inference cannot be made by inspecting the measurements from one of the links alone, except in the extreme situation in which that link carries no traffic at all. Thus it is necessary to transport the measurements from one of the links to the other, or to transport both measurements to a third location. The measured data is potentially high-rate, however, so this transportation may require that the data be compressed. This raises the question of how to compress data when the goal is not to reproduce it *per se*, but rather to perform inference. A similar problem arises when inferring the speed of a moving vehicle from the times that it passes certain waypoints.

These problems can be modeled mathematically by the setup depicted in Fig. 1, which we call the  $L$ -encoder general hypothesis testing problem. A vector source  $(X_1, \dots, X_L, Y)$  has different joint distributions  $P_{X_1, \dots, X_L, Y}$  and  $Q_{X_1, \dots, X_L, Y}$  under two hypotheses  $H_0$  and  $H_1$ , respectively. Encoder  $l$  observes an i.i.d. string distributed according to  $X_l$  and sends a message to the detector at a finite rate of  $R_l$  bits per observation using a noiseless channel. The detector, which has access to an i.i.d. string distributed according to  $Y$ , makes a decision between the hypotheses. The detector may make two types of error: the type 1 error ( $H_0$  is true but the detector decides otherwise) and the type 2 error ( $H_1$  is true but the detector decides otherwise). The type 1 error probability is upper bounded by a fixed value. The type 2 error probability decreases exponentially fast, say with an exponent  $E$ , as the length of the i.i.d. strings increases. The goal is to characterize the rate-exponent region of the problem, which is the set of all achievable rate-exponent vectors  $(R_1, \dots, R_L, E)$ , in the regime in which the type 1 error probability is small. This problem was first introduced by Berger [3] (see also [4]) and arises naturally in many applications. Yet despite these applications, the theoretical understanding of this problem is far from complete,

<sup>\*</sup>Both authors are with the School of Electrical and Computer Engineering, Cornell University, Ithaca, NY, 14853, USA. (Email: mr534@cornell.edu, wagner@ece.cornell.edu.)

especially when compared with its sibling, distributed source coding, where random binning has been shown to be a key ingredient in many optimal schemes.

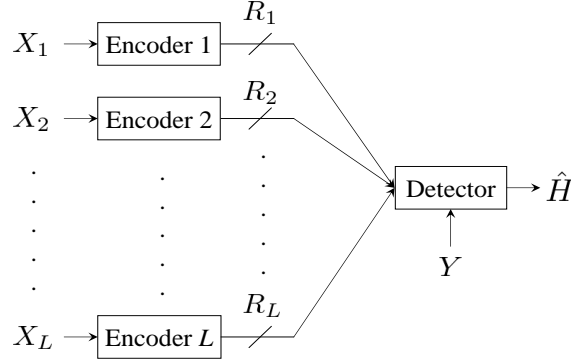


Figure 1:  $L$ -encoder general hypothesis testing

Note that if one of the variables in the set  $(X_1, \dots, X_L, Y)$  has a different marginal distribution under  $P_{X_1, \dots, X_L, Y}$  and  $Q_{X_1, \dots, X_L, Y}$ , then one of the terminals can detect the underlying hypothesis with an exponentially-decaying type 2 error probability, even without receiving any information from the other terminals, and could communicate this decision to other terminals by broadcasting a single bit. Motivated by the applications mentioned above, we shall focus our attention on the case in which the variables  $X_1, \dots, X_L, Y$  have the same marginal distributions under both hypotheses.

Ahlsvede and Csiszár [5] studied a special case of this problem in which  $L = 1$ . They presented a scheme in which the encoder sends a quantized value of  $X_1$  to the detector which uses it to perform the test with the help of  $Y$ . They showed that their scheme is optimal for a “test against independence.” Their scheme was later improved by Han [6] and Shimokawa-Han-Amari [7]. In the latter improvement, the encoder first quantizes  $X_1$ , then bins the quantized value using a Slepian and Wolf encoder [8]. The detector first decodes the quantized value with the help of  $Y$  and then performs a likelihood ratio test. In this scheme, type 2 errors can occur in two different ways: the binning can fail so that the receiver decodes the wrong codeword and therefore makes an incorrect decision, or the true codeword can be decoded correctly yet be atypically distributed with  $Y$ , again resulting in an incorrect decision. Moreover, there is a tension between these two forms of error. If the codeword is a high fidelity representation of  $X_1$ , then binning errors are likely, yet the detector is relatively unlikely to make an incorrect decision if it decodes the codeword correctly. If the codeword is a low fidelity representation, then binning errors are unlikely, but the detector is more likely to make an incorrect decision when it decodes correctly.

Fig. 2 illustrates this tradeoff for a fixed test channel  $P_{U_1|X_1}$  used for quantization. All mutual information quantities are computed with respect to  $P$ .  $\rho_2^*(U_1)$  and  $\rho_1^*(U_1)$  are the exponents associated with type 2 errors due to binning errors and assuming correct decoding of the codeword, respectively. Formulas for each are available in [4]. For low rates, binning errors are common and  $\rho_2^*(U_1)$  dominates the overall exponent. For high rates, binning errors are uncommon and  $\rho_1^*(U_1)$  dominates the overall exponent. To achieve the overall performance, the test channel should be chosen so that these two exponents are equal; if they are not, then making the test channel slightly more or less noisy will yield better performance. A similar tradeoff arises in the analysis of error exponents of binning-based schemes for the Wyner-Ziv problem [9, 10, 11, 12] and in the design of short block-length codes for Wyner-Ziv or joint source-channel coding. Evidently the benefit accrued from binning is reduced when one considers error exponents, as opposed to when the design criterion is vanishing error probability or average distortion, because the error exponent associated with the binning process itself may dominate the overall performance.

The Shimokawa-Han-Amari scheme uses random, unstructured binning. It is known from the lossless source coding literature that structured binning schemes can strictly improve upon unstructured binning schemes in terms of the error expo-

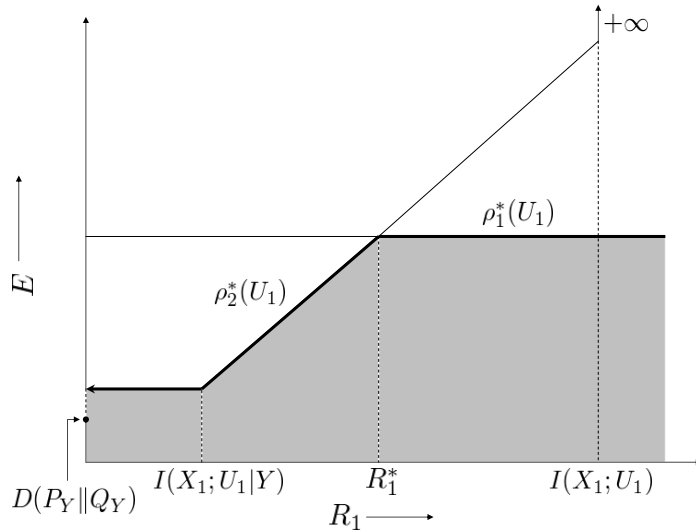


Figure 2: Shimokawa-Han-Amari achievable region for a fixed channel  $P_{U_1|X_1}$

nents [13, 14, 15]. Thus, two questions naturally arise:

1. Is the tradeoff depicted in Fig. 2 fundamental to the problem or an artifact of a suboptimal scheme?
2. Can the scheme be improved by using structured binning?

We conclusively answer both questions and show that unstructured binning is optimal in several important cases. We begin by considering a special case of the problem that we call  $L$ -encoder hypothesis testing against conditional independence. Here  $Y$  is replaced by a three-source  $(X_{L+1}, Y, Z)$  such that  $Z$  induces conditional independence between  $(X_1, \dots, X_L, X_{L+1})$  and  $Y$  under  $H_1$ . In addition,  $(X_1, \dots, X_L, X_{L+1}, Z)$  and  $(Y, Z)$  have the same distributions under both hypotheses. This problem is a generalization of the single-encoder test against independence studied by Ahlswede and Csiszár [5],

For this problem we provide an achievable region, based on a scheme we call Quantize-Bin-Test, that reduces to the Shimokawa-Han-Amari region for  $L = 1$  yet is significantly simpler. We also introduce an outer bound similar to the outer bound for the distributed rate-distortion problem given by Wagner and Anantharam [16]. The idea is to introduce an auxiliary random variable that induces conditional independence between the sources. This technique of obtaining an outer bound has been used to prove results in many distributed source coding problems [16, 17, 18, 19, 20, 21].

The inner (achievable) and outer bounds are shown to match in three examples. The first is the case in which there is only one encoder ( $L = 1$ ). Although this problem is simply the conditional version of the test against independence studied by Ahlswede and Csiszár [5], the conditional version is much more complicated due to the necessary introduction of binning. It follows that the Shimokawa-Han-Amari scheme is optimal for  $L = 1$ , providing what appears to be the first nontrivial optimality result for this scheme. This problem arises in detecting network flows in the presence of common cross-traffic that is known to the detector. Here  $X_1$  represents the network traffic measured at a remote location,  $Y$  is the traffic measured at the detector, and  $Z$  represents the cross-traffic. The goal is to detect the presence of common traffic beyond  $Z$ , i.e., to determine whether  $Z$  captures all of the dependence between  $X_1$  and  $Y$ .

The second is a problem inspired by a result of Gel'fand and Pinsker [22]. We refer to this as the Gel'fand and Pinsker hypothesis testing against independence problem, the setup of which is shown in Fig. 3. Here  $X_{L+1}$  and  $Z$  are deterministic and there is a source  $X$  which under  $H_0$  is the minimum sufficient statistic for  $Y$  given  $(X_1, \dots, X_L)$  such that  $X_1, \dots, X_L, Y$  are conditionally independent given  $X$ . We characterize the set of rate vectors  $(R_1, \dots, R_L)$  that achieve the centralized exponent  $I(X; Y)$ . We show that the Quantize-Bin-Test scheme is optimal for this problem.

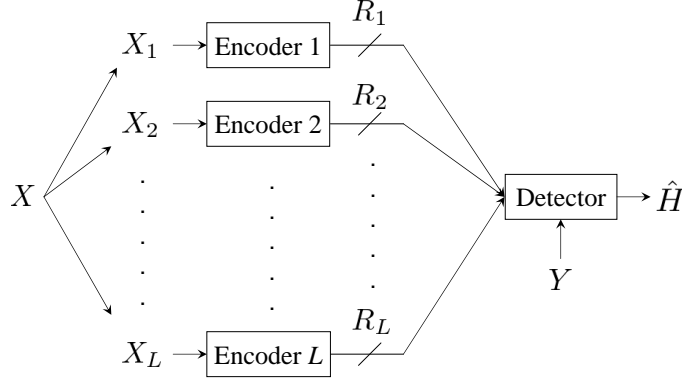


Figure 3: Gel'fand and Pinsker hypothesis testing against independence

The third is the Gaussian many-help-one hypothesis testing against independence problem, the setup of which is shown in Fig. 4. Here the sources are jointly Gaussian and there is another scalar Gaussian source  $X$  observed by the main encoder which sends a message to the detector at a rate  $R$ . The encoder observing  $X_l$  is now referred to as the helper  $l$ . We characterize the rate-exponent region of this problem in a special case when  $X_1, \dots, X_L, Y$  are conditionally independent given  $X$ . We use results on related source coding problem by Oohama [23] and Prabhakaran *et al.* [24] to obtain an outer bound, which we show is achieved by the Quantize-Bin-Test scheme.

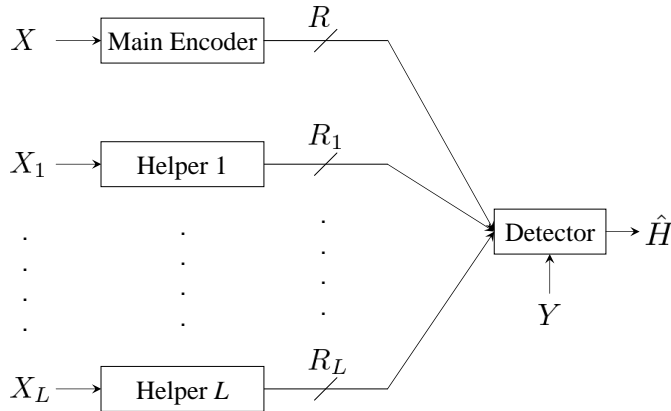


Figure 4: Gaussian many-help-one hypothesis testing against independence

For all three examples, we obtain the solution by observing that the relevant error exponent takes the form of a mutual information, and thereby relate the problem to a source-coding problem. This correspondence was first observed by Ahlswede and Csiszár [5]. Tian and Chen later applied it in the context of successive refinement [25]. These three conclusive results enable us to answer both of the above questions. Because the Shimokawa-Han-Amari scheme is optimal for  $L = 1$ , the tradeoff that it entails, depicted in Fig. 2, must be fundamental to the problem. Moreover, as both the Shimokawa-Han-Amari and Quantize-Bin-Test schemes do not use structured binning, we conclude that it is not necessary for this problem, at least in the special case considered here.

As a byproduct of our results, we obtain an outer bound for a more general class of instances of the distributed hypothesis testing problem. This is the first nontrivial outer bound for the problem, and numerical experiments show that it is quite close

to the existing achievable regions in many cases.

The rest of the paper is organized as follows. In Section 2, we introduce the notation used in the paper. We give the mathematical formulation of the  $L$ -encoder general hypothesis testing problem in Section 3. Section 4 is devoted to the  $L$ -encoder hypothesis testing against conditional independence problem. Section 5 is on the special case in which there is only one encoder. The Gel'fand and Pinsker hypothesis testing against independence problem is studied in Section 6. The Gaussian many-help-one hypothesis testing against independence problem is studied on Section 7. Finally, we present the outer bound for a class of the general problem in Section 8.

## 2 Notation

We use upper case to denote random variables and vectors. Boldface is used to distinguish vectors from scalars. Arbitrary realizations of random variables and vectors are denoted in lower case. For a random variable  $X$ ,  $X^n$  denotes an i.i.d. vector of length  $n$ ,  $X^n(i)$  denotes its  $i$ th component,  $X^n(i : j)$  denotes the  $i$ th through  $j$ th components, and  $X^n(i^c)$  denotes all but the  $i$ th component. For random variables  $X$  and  $Y$ , we use  $\sigma_X^2$  and  $\sigma_{X|Y}^2$  to denote the variance of  $X$  and the conditional variance of  $X$  given  $Y$ , respectively. The closure of a set  $\mathcal{A}$  is denoted by  $\overline{\mathcal{A}}$ .  $|f|$  denotes the cardinality of the range of a function  $f$ .  $1_A$  denotes the indicator function of an event  $A$ . The determinant of a matrix  $\mathbf{K}$  is denoted by  $\det(\mathbf{K})$ . The notation  $x^+$  denotes  $\max(x, 0)$ . All logarithms are to the base 2.  $\mathbb{R}_+^L$  is used to denote the positive orthant in  $L$ -dimensional Euclidean space. The notation  $X \leftrightarrow Y \leftrightarrow Z$  means that  $X, Y$ , and  $Z$  form a Markov chain in this order. For  $0 \leq p \leq 1$ ,  $H_b(p)$  denotes the binary entropy function defined as

$$H_b(p) \triangleq -p \log p - (1-p) \log(1-p).$$

All entropy and mutual information quantities are under the null hypothesis,  $H_0$ , unless otherwise stated.

## 3 $L$ -Encoder General Hypothesis Testing

### 3.1 Problem Formulation

Let  $(X_1, \dots, X_L, Y)$  be a generic source taking values in  $\prod_{l=1}^L \mathcal{X}_l \times \mathcal{Y}$ , where  $\mathcal{X}_1, \dots, \mathcal{X}_L$ , and  $\mathcal{Y}$  are alphabet sets of  $X_1, \dots, X_L$ , and  $Y$ , respectively. The distribution of the source is  $P_{X_1 \dots X_L Y}$  under the null hypothesis  $H_0$  and is  $Q_{X_1 \dots X_L Y}$  under the alternate hypothesis  $H_1$ , i.e.,

$$H_0 : P_{X_1 \dots X_L Y}$$

$$H_1 : Q_{X_1 \dots X_L Y}.$$

Let  $\{(X_1^n(i), \dots, X_L^n(i), Y^n(i))\}_{i=1}^n$  be an i.i.d. sequence of random vectors with the distribution at a single stage same as that of  $(X_1, \dots, X_L, Y)$ . We use  $\mathcal{L}$  to denote the set  $\{1, \dots, L\}$ . For  $S \subseteq \mathcal{L}$ ,  $S^c$  denotes the complement set  $\mathcal{L} \setminus S$  and  $\mathbf{X}_S^n(i)$  denotes  $(X_l^n(i))_{l \in S}$ . When  $S = \mathcal{L}$ , we simply write  $\mathbf{X}_{\mathcal{L}}^n(i)$  as  $\mathbf{X}^n(i)$ . Likewise when  $S = \{l\}$ , we write  $\mathbf{X}_{\{l\}}^n(i)$  and  $\mathbf{X}_{\{l\}^c}^n(i)$  as  $X_l^n(i)$  and  $\mathbf{X}_{l^c}^n(i)$ , respectively. Similar notation will be used for other collections of random variables.

As depicted in Fig. 1, the encoder  $l$  observes  $X_l^n$ , then sends a message to the detector using an encoding function

$$f_l^{(n)} : \mathcal{X}_l^n \mapsto \{1, \dots, M_l^{(n)}\}.$$

$Y^n$  is available at the detector, which uses it and the messages from the encoders to make a decision between the hypotheses based on a decision rule

$$g^{(n)}(m_1, \dots, m_L, y^n) = \begin{cases} H_0 & \text{if } (m_1, \dots, m_L, y^n) \text{ is in } A \\ H_1 & \text{otherwise,} \end{cases}$$

where

$$A \subseteq \prod_{l=1}^L \{1, \dots, M_l^{(n)}\} \times \mathcal{Y}^n$$

is the acceptance region for  $H_0$ . The encoders  $f_l^{(n)}$  and the detector  $g^{(n)}$  are such that the type 1 error probability does not exceed a fixed  $\epsilon$  in  $(0, 1)$ , i.e.,

$$P_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}}} Y^n(A^c) \leq \epsilon,$$

and the type 2 error probability does not exceed  $\eta$ , i.e.,

$$Q_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}}} Y^n(A) \leq \eta.$$

**Definition 1.** A rate-exponent vector

$$(\mathbf{R}, E) = (R_1, \dots, R_L, E)$$

is achievable for a fixed  $\epsilon$  if for any positive  $\delta$  and sufficiently large  $n$ , there exists encoders  $f_l^{(n)}$  and a detector  $g^{(n)}$  such that

$$\begin{aligned} \frac{1}{n} \log M_l^{(n)} &\leq R_l + \delta \text{ for all } l \text{ in } \mathcal{L}, \text{ and} \\ -\frac{1}{n} \log \eta &\geq E - \delta. \end{aligned}$$

Let  $\mathcal{R}_\epsilon$  be the set of all achievable rate-exponent vectors for a fixed  $\epsilon$ . The rate-exponent region  $\mathcal{R}$  is defined as

$$\mathcal{R} \triangleq \bigcap_{\epsilon > 0} \mathcal{R}_\epsilon.$$

Our goal is to characterize the region  $\mathcal{R}$ .

### 3.2 Entropy Characterization of the Rate-Exponent Region

We start with the entropy characterization of the rate-exponent region. We shall use it later in the paper to obtain inner and outer bounds. Define the set

$$\mathcal{R}_* \triangleq \bigcup_n \bigcup_{(f_l^{(n)})_{l \in \mathcal{L}}} \mathcal{R}_*\left(n, (f_l^{(n)})_{l \in \mathcal{L}}\right),$$

where

$$\begin{aligned} \mathcal{R}_*\left(n, (f_l^{(n)})_{l \in \mathcal{L}}\right) &\triangleq \left\{ (\mathbf{R}, E) : R_l \geq \frac{1}{n} \log |f_l^{(n)}(X_l^n)| \text{ for all } l \text{ in } \mathcal{L}, \text{ and} \right. \\ &\quad \left. E \leq \frac{1}{n} D\left(P_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}}} Y^n \parallel Q_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}}} Y^n\right) \right\}. \end{aligned} \quad (1)$$

We have the following Proposition.

**Proposition 1.**  $\mathcal{R} = \overline{\mathcal{R}_*}$ .

The proof of Proposition 1 is a straight-forward generalization of that of Theorem 1 in [5] and is hence omitted. Ahlswede and Csiszár [5] showed that for  $L = 1$ , the strong converse holds, i.e.,  $\mathcal{R}_\epsilon$  is independent of  $\epsilon$ . Thus,  $\overline{\mathcal{R}_*}$  is essentially a characterization for both  $\mathcal{R}$  and  $\mathcal{R}_\epsilon$ . While we expect this to hold for the problem under investigation too, we shall not investigate it here. We next study a class of instances of the problem before returning to the general problem in Section 8.

## 4 $L$ -Encoder Hypothesis Testing against Conditional Independence

We consider a class of instances of the general problem, referred to as the  $L$ -encoder hypothesis testing against conditional independence problem, and obtain inner and outer bounds to the rate-exponent region. These bounds coincide and characterize the region completely in some cases. Moreover, the outer bound for this problem can be used to give an outer bound for a more general class of problems, as we shall see later.

Let  $X_{L+1}$  and  $Z$  be two generic sources taking values in alphabet sets  $\mathcal{X}_{L+1}$  and  $\mathcal{Z}$ , respectively such that  $(\mathbf{X}, X_{L+1})$  and  $Y$  are conditionally independent given  $Z$  under  $H_1$ , and the distributions of  $(\mathbf{X}, X_{L+1}, Z)$  and  $(Y, Z)$  are the same under both hypotheses, i.e.,

$$\begin{aligned} H_0 &: P_{\mathbf{X}X_{L+1}Y|Z}P_Z \\ H_1 &: P_{\mathbf{X}X_{L+1}|Z}P_{Y|Z}P_Z. \end{aligned}$$

The problem formulation is the same as before with  $Y$  replaced by  $(X_{L+1}, Z, Y)$  in it. The reason for focusing on this special case is that the relative entropy in (1) becomes a mutual information, which simplifies the analysis. Let  $\mathcal{R}^{CI}$  be the rate-exponent region of this problem. Here “ $CI$ ” stands for conditional independence. Let

$$\mathcal{R}_*^{CI} \triangleq \bigcup_n \bigcup_{(f_l^{(n)})_{l \in \mathcal{L}}} \mathcal{R}_*^{CI} \left( n, (f_l^{(n)})_{l \in \mathcal{L}} \right),$$

where

$$\begin{aligned} \mathcal{R}_*^{CI} \left( n, (f_l^{(n)})_{l \in \mathcal{L}} \right) &\triangleq \left\{ (\mathbf{R}, E) : R_l \geq \frac{1}{n} \log \left| f_l^{(n)}(X_l^n) \right| \text{ for all } l \text{ in } \mathcal{L}, \text{ and} \right. \\ &\quad \left. E \leq \frac{1}{n} I \left( (f_l^{(n)}(X_l^n))_{l \in \mathcal{L}}, X_{L+1}^n; Y^n \middle| Z^n \right) \right\}. \end{aligned}$$

We have the following corollary as a consequence of Proposition 1.

**Corollary 1.**  $\mathcal{R}^{CI} = \overline{\mathcal{R}_*^{CI}}$ .

With mutual information replacing relative entropy, the problem can be analyzed using techniques from distributed rate-distortion. In particular, both inner and outer bounds for that problem can be applied here.

### 4.1 Quantize-Bin-Test Inner Bound

Our inner bound is based on a simple scheme which we call the Quantize-Bin-Test scheme. In this scheme, encoders, as in the Shimokawa-Han-Amari scheme, quantize and then bin their observations, but the detector now performs the test directly using the bins. The inner bound obtained is similar to the generalized Berger-Tung inner bound for distributed source coding [26, 27, 28]. Let  $\Lambda_i$  be the set of finite-alphabet random variables  $\lambda_i = (U_1, \dots, U_L, T)$  satisfying

(C1)  $T$  is independent of  $(\mathbf{X}, X_{L+1}, Y, Z)$ , and

(C2)  $U_l \leftrightarrow (X_l, T) \leftrightarrow (\mathbf{U}_{l^c}, \mathbf{X}_{l^c}, X_{L+1}, Y, Z)$  for all  $l$  in  $\mathcal{L}$ .

Define the set

$$\begin{aligned} \mathcal{R}_i^{CI}(\lambda_i) &\triangleq \left\{ (\mathbf{R}, E) : \sum_{l \in S} R_l \geq I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c}, X_{L+1}, Z, T) \text{ for all } S \subseteq \mathcal{L}, \text{ and} \right. \\ &\quad \left. E \leq I(Y; \mathbf{U}, X_{L+1} | Z, T) \right\} \end{aligned}$$

and let

$$\mathcal{R}_i^{CI} \triangleq \bigcup_{\lambda_i \in \Lambda_i} \mathcal{R}_i^{CI}(\lambda_i).$$

The following lemma asserts that  $\mathcal{R}_i^{CI}$  is computable and closed.

**Lemma 1.** (a)  $\mathcal{R}_i^{CI}$  remains unchanged if we impose the following cardinality bound on  $(\mathbf{U}, T)$  in  $\Lambda_i$

$$|\mathcal{U}_l| \leq |\mathcal{X}_l| + 2^L - 1 \text{ for all } l \text{ in } \mathcal{L}, \text{ and} \\ |\mathcal{T}| \leq 2^L.$$

(b)  $\mathcal{R}_i^{CI}$  is closed.

The proof of Lemma 1 is presented in Appendix A. Although the cardinality bound is exponential in the number of encoders, one can obtain an improved bound by exploiting the contra-polymatroid structure of  $\mathcal{R}_i^{CI}$  [29, 30]. We do not do so here because it is technically involved and we just want to prove that  $\mathcal{R}_i^{CI}$  is closed. The following theorem gives an inner bound to the rate-exponent region.

**Theorem 1.**  $\mathcal{R}_i^{CI} \subseteq \mathcal{R}^{CI}$ .

Theorem 1 is proved in Appendix B.

*Remark 1:* Although our inner bound is stated for the special case of the test against conditional independence, it can be extended to the general case. But, the inner bound thus obtained will be quite complicated, with competing exponents, and it is not needed in this paper.

It is worth pointing out that the Quantize-Bin-Test scheme is in general suboptimal for problems in which encoders' observations have common randomness, i.e., there exists deterministic functions of encoders' observations that is common to encoders. However, it is straightforward to generalize this scheme by using the idea from the common-component scheme for distributed source coding problems [31].

## 4.2 Outer Bound

The outer bound is similar to the outer bound for the distributed rate-distortion problem given by Wagner and Anantharam [16]. Let  $\Lambda_o$  be the set of finite-alphabet random variables  $\lambda_o = (\mathbf{U}, W, T)$  satisfying

(C3)  $(W, T)$  is independent of  $(\mathbf{X}, X_{L+1}, Y, Z)$ , and

(C4)  $U_l \leftrightarrow (X_l, W, T) \leftrightarrow (\mathbf{U}_{l^c}, \mathbf{X}_{l^c}, X_{L+1}, Y, Z)$  for all  $l$  in  $\mathcal{L}$ ,

and let  $\chi$  be the set of finite-alphabet random variable  $X$  such that  $X_1, \dots, X_L, X_{L+1}, Y$  are conditionally independent given  $(X, Z)$ . Note that  $\chi$  is nonempty because it contains  $(\mathbf{X}, X_{L+1})$ . For a given  $X$  in  $\chi$  and  $\lambda_o$  in  $\Lambda_o$ , the joint distribution of  $X$ ,  $(\mathbf{X}, X_{L+1}, Y, Z)$ , and  $\lambda_o$  satisfy the Markov condition

$$X \leftrightarrow (\mathbf{X}, X_{L+1}, Y, Z) \leftrightarrow \lambda_o.$$

Wagner and Anantharam [16] refer to this condition as “Markov coupling” between  $X$  and  $\lambda_o$ . Define the set

$$\mathcal{R}_o^{CI}(X, \lambda_o) \triangleq \left\{ (\mathbf{R}, E) : \sum_{l \in S} R_l \geq I(X; \mathbf{U}_S | \mathbf{U}_{S^c}, X_{L+1}, Z, T) + \sum_{l \in S} I(X_l; U_l | X, W, X_{L+1}, Z, T) \text{ for all } S \subseteq \mathcal{L}, \text{ and} \right. \\ \left. E \leq I(Y; \mathbf{U}, X_{L+1} | Z, T) \right\}.$$

Also let

$$\mathcal{R}_o^{CI} \triangleq \bigcap_{X \in \chi} \bigcup_{\lambda_o \in \Lambda_o} \mathcal{R}_o^{CI}(X, \lambda_o).$$

We have the following outer bound to the rate-exponent region.

**Theorem 2.**  $\mathcal{R}_*^{CI} \subseteq \mathcal{R}_o^{CI}$  and therefore  $\mathcal{R}^{CI} \subseteq \overline{\mathcal{R}_o^{CI}}$ .

The proof of the first inclusion is presented in Appendix C. The first inclusion and Corollary 1 imply the second inclusion. The next three sections provide examples in which the inner and outer bounds coincide. In Section 8, we will see how to extend the outer bound to the general problem.

## 5 1-Encoder Hypothesis Testing against Conditional Independence

In this section, we study a special case in which  $L = 1$ . We prove that the Quantize-Bin-Test scheme is optimal for this problem. We also prove that the Shimokawa-Han-Amari inner bound coincides with the Quantize-Bin-Test inner bound, establishing that the Shimokawa-Han-Amari scheme is also optimal.

### 5.1 Rate-Exponent Region

**Theorem 3.** *For this problem, the rate-exponent region*

$$\mathcal{R}^{CI} = \overline{\mathcal{R}_o^{CI}} = \mathcal{R}_i^{CI} \tag{2}$$

$$\begin{aligned} &= \tilde{\mathcal{R}}^{CI} \triangleq \left\{ (R_1, E) : \text{there exists } U_1 \text{ such that} \right. \\ &\quad R_1 \geq I(X_1; U_1 | X_2, Z), \\ &\quad E \leq I(Y; U_1, X_2 | Z), \\ &\quad |\mathcal{U}_1| \leq |\mathcal{X}_1| + 1, \text{ and} \\ &\quad \left. U_1 \leftrightarrow X_1 \leftrightarrow (X_2, Y, Z) \right\}. \end{aligned} \tag{3}$$

*Proof.* To show (2), it suffices to show that

$$\mathcal{R}_o^{CI} \subseteq \mathcal{R}_i^{CI},$$

because  $\mathcal{R}_i^{CI}$  is closed from Lemma 1(b). Consider  $(R_1, E)$  in  $\mathcal{R}_o^{CI}$ . Take  $X = X_2$ . It is evident that  $X_2$  is in  $\chi$ . Then there exists  $\lambda_o = (U_1, W, T)$  in  $\Lambda_o$  such that  $(R_1, E)$  is in  $\mathcal{R}_o^{CI}(X_2, \lambda_o)$ , i.e.,

$$\begin{aligned} R_1 &\geq I(X_2; U_1 | X_2, Z, T) + I(X_1; U_1 | X_2, Z, W, T) \\ &= I(X_1; U_1 | X_2, Z, W, T), \end{aligned}$$

and

$$\begin{aligned} E &\leq I(Y; U_1, X_2 | Z, T) \\ &= H(Y | Z, T) - H(Y | U_1, X_2, Z, T) \\ &\leq H(Y | Z, W, T) - H(Y | U_1, X_2, Z, W, T) \\ &= I(Y; U_1, X_2 | Z, W, T), \end{aligned} \tag{4}$$

where (4) follows from conditioning reduces entropy and the fact that  $(Y, Z)$  is independent of  $(W, T)$ . If we set  $\tilde{T} = (W, T)$ , then it is easy to verify that  $\lambda_i = (U_1, \tilde{T})$  is in  $\Lambda_i$  and we have

$$R_1 \geq I(X_1; U_1 | X_2, Z, \tilde{T}), \text{ and} \quad (5)$$

$$E \leq I(Y; U_1, X_2 | Z, \tilde{T}). \quad (6)$$

Therefore,  $(R_1, E)$  is in  $\mathcal{R}_i^{CI}(\lambda_i)$ , which implies that  $(R_1, E)$  is in  $\mathcal{R}_i^{CI}$ . This completes the proof of (2).

To prove (3), it suffices to show that

$$\mathcal{R}_i^{CI} \subseteq \tilde{\mathcal{R}}^{CI}.$$

The reverse containment immediately follows if we restrict  $T$  to be deterministic in the definition of  $\mathcal{R}_i^{CI}$ . Continuing from the proof of (2), let  $\tilde{U}_1 = (U_1, \tilde{T})$ . Since  $(U_1, \tilde{T})$  is in  $\Lambda_i$ , we have that  $\tilde{T}$  is independent of  $(X_1, X_2, Y, Z)$  and that

$$U_1 \leftrightarrow (\tilde{T}, X_1) \leftrightarrow (X_2, Y, Z).$$

Both together imply that

$$\tilde{U} \leftrightarrow X_1 \leftrightarrow (X_2, Y, Z).$$

We next have from (5) that

$$\begin{aligned} R_1 &\geq I(X_1; U_1 | X_2, Z, \tilde{T}) \\ &= I(X_1; U_1 | X_2, Z, \tilde{T}) + I(X_1; \tilde{T} | X_2, Z) \\ &= I(X_1; U_1, \tilde{T} | X_2, Z) \\ &= I(X_1; \tilde{U}_1 | X_2, Z), \end{aligned} \quad (7)$$

where (7) follows because  $\tilde{T}$  is independent of  $(X_1, X_2, Y, Z)$ . And (6) similarly yields

$$E \leq I(Y; \tilde{U}_1, X_2 | Z).$$

Using the support lemma [32, Lemma 3.4, pp. 310] as in the proof of Lemma 1(a), we can obtain the cardinality bound

$$|\tilde{\mathcal{U}}_1| \leq |\mathcal{X}_1| + 1.$$

We thus conclude that  $(R_1, E)$  is in  $\tilde{\mathcal{R}}^{CI}$ . □

## 5.2 Optimality of Shimokawa-Han-Amari Scheme

The Shimokawa-Han-Amari scheme operates as follows. Consider a test channel  $P_{U_1|X_1}$ , a sufficiently large block length  $n$ , and  $\alpha > 0$ . Let  $\bar{R}_1 = I(X_1; U_1) + \alpha$ . To construct the codebook, we first generate  $2^{n\bar{R}_1}$  independent codewords  $U_1^n$ , each according to  $\prod_{i=1}^n P_{U_1}(u_{1i})$ , and then distribute them uniformly into  $2^{nR_1}$  bins. The codebook and the bin assignment are revealed to the encoder and the detector. The encoder first quantizes  $X_1^n$  by selecting a codeword  $U_1^n$  that is jointly typical with it. With high probability, there will be at least one such codeword. The encoder then sends to the detector the index of the bin to which the codeword  $U_1^n$  belongs. The joint type of  $(X_1^n, U_1^n)$  is also sent to the detector, which requires zero additional rate asymptotically. The detector finds a codeword  $\hat{U}_1^n$  in the bin that minimizes the empirical entropy  $H(U_1^n, Y^n)$ . It then performs the test and declares  $H_0$  if and only if both  $(X_1^n, U_1^n)$  and  $(Y^n, \hat{U}_1^n)$  are jointly typical under  $H_0$ . The inner bound thus obtained is as follows. Define

$$\begin{aligned} \mathcal{A}(R_1) &\triangleq \left\{ U_1 : R_1 \geq I(X_1; U_1 | X_2, Y, Z), \quad U_1 \leftrightarrow X_1 \leftrightarrow (X_2, Y, Z), \text{ and } |\mathcal{U}_1| \leq |\mathcal{X}_1| + 1 \right\} \\ \mathcal{B}(U_1) &\triangleq \left\{ P_{\tilde{U}_1 \tilde{X}_1 \tilde{X}_2 \tilde{Y} \tilde{Z}} : P_{\tilde{U}_1 \tilde{X}_1} = P_{U_1 X_1} \text{ and } P_{\tilde{U}_1 \tilde{X}_2 \tilde{Y} \tilde{Z}} = P_{U_1 X_2 Y Z} \right\} \\ \mathcal{C}(U_1) &\triangleq \left\{ P_{\tilde{U}_1 \tilde{X}_1 \tilde{X}_2 \tilde{Y} \tilde{Z}} : P_{\tilde{U}_1 \tilde{X}_1} = P_{U_1 X_1}, \quad P_{\tilde{X}_2 \tilde{Y} \tilde{Z}} = P_{X_2 Y Z}, \text{ and } H(\tilde{U}_1 | \tilde{X}_2, \tilde{Y}, \tilde{Z}) \geq H(U_1 | X_2, Y, Z) \right\}. \end{aligned}$$

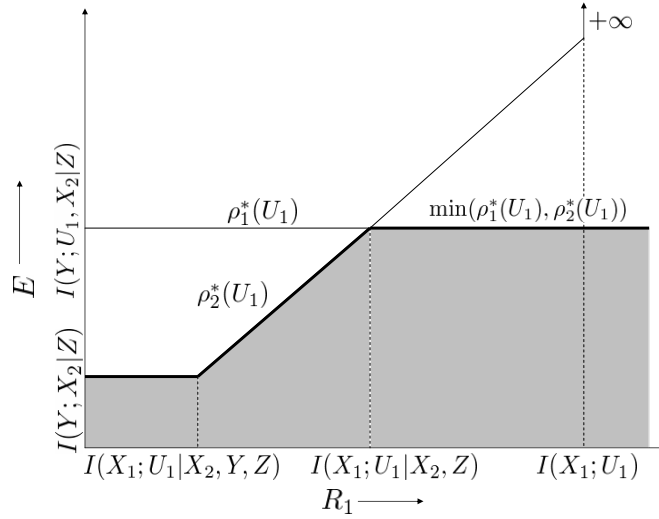


Figure 5: Shimokawa-Han-Amari achievable region for a fixed  $P_{U_1|X_1}$

In addition, define the exponents

$$\begin{aligned}\rho_1^*(U_1) &\triangleq \min_{P_{\tilde{U}_1 \tilde{X}_1 \tilde{X}_2 \tilde{Y} \tilde{Z}} \in \mathcal{B}(U_1)} D(P_{\tilde{U}_1 \tilde{X}_1 \tilde{X}_2 \tilde{Y} \tilde{Z}} \| P_{U_1|X_1} P_{X_1 X_2|Z} P_{Y|Z} P_Z) \\ \rho_2^*(U_1) &\triangleq \begin{cases} +\infty & \text{if } R_1 \geq I(U_1; X_1) \\ \rho_2(U_1) & \text{otherwise} \end{cases} \\ \rho_2(U_1) &\triangleq [R_1 - I(X_1; U_1|X_2, Y, Z)]^+ + \min_{P_{\tilde{U}_1 \tilde{X}_1 \tilde{X}_2 \tilde{Y} \tilde{Z}} \in \mathcal{C}(U_1)} D(P_{\tilde{U}_1 \tilde{X}_1 \tilde{X}_2 \tilde{Y} \tilde{Z}} \| P_{U_1|X_1} P_{X_1 X_2|Z} P_{Y|Z} P_Z).\end{aligned}$$

Finally, define

$$E_{SHA}(R_1) \triangleq \max_{U_1 \in \mathcal{A}(R_1)} \min(\rho_1^*(U_1), \rho_2^*(U_1)).$$

Recall that  $\rho_2^*(U_1)$  and  $\rho_1^*(U_1)$  are the exponents associated with type 2 errors due to binning errors and assuming correct decoding of the codeword, respectively.

**Theorem 4.** [7]  $(R_1, E)$  is in the rate-exponent region if

$$E \leq E_{SHA}(R_1).$$

Fig. 5 shows the Shimokawa-Han-Amari achievable exponent as a function of the rate assuming a fixed channel  $P_{U_1|X_1}$  is used for quantization. This is simply Fig. 2 particularized to the 1-encoder hypothesis testing against conditional independence problem. For rates  $R_1 \geq I(X_1, U_1|X_2, Z)$ ,  $\rho_1^*(U_1)$  dominates  $\rho_2^*(U_1)$  and there is no penalty for binning at these rates as the exponent stays the same. Therefore, we can bin all the way down to the rate  $R_1 = I(X_1, U_1|X_2, Z)$  without any loss in the exponent. However, if we bin further at rates  $R_1$  in  $[I(X_1, U_1|X_2, Y, Z), I(X_1, U_1|X_2, Z))$ , then  $\rho_2^*(U_1)$  dominates  $\rho_1^*(U_1)$ , the exponent decreases linearly with  $R_1$ , and the performance deteriorates all the way down to a point at which the message from the encoder is useless. At this point, the binning rate  $R_1$  equals  $I(X_1, U_1|X_2, Y, Z)$  and the exponent equals  $I(Y; X_2|Z)$ , which is the exponent when the detector ignores the encoder's message. This competition between the exponents makes the optimality of the Shimokawa-Han-Amari scheme unclear. We prove that it is indeed optimal by showing that the Shimokawa-Han-Amari inner bound simplifies to the Quantize-Bin-Test inner bound, which by Theorem 3 is tight. Let us define

$$\mathcal{A}^*(R_1) \triangleq \left\{ U_1 : R_1 \geq I(X_1; U_1|X_2, Z), \quad U_1 \leftrightarrow X_1 \leftrightarrow (X_2, Y, Z), \text{ and } |\mathcal{U}_1| \leq |\mathcal{X}_1| + 1 \right\}$$

and

$$E_{QBT}(R_1) \triangleq \max_{U_1 \in \mathcal{A}^*(R_1)} I(Y; U_1, X_2 | Z).$$

We have the following theorem.

**Theorem 5.** *If  $(R_1, E)$  is in the rate-exponent region, then*

$$E \leq E_{QBT}(R_1) = E_{SHA}(R_1).$$

*Proof.* The inequality follows from Theorem 3. To prove the equality, it is sufficient to show that

$$E_{SHA}(R_1) \geq E_{QBT}(R_1).$$

The reverse inequality follows from Theorem 3 and 4. Since conditioning reduces entropy and any  $U_1$  in  $\mathcal{A}^*(R_1)$  satisfies the Markov chain

$$U_1 \leftrightarrow X_1 \leftrightarrow (X_2, Y, Z),$$

we have

$$\begin{aligned} R_1 &\geq I(X_1; U_1 | X_2, Z) \\ &= H(U_1 | X_2, Z) - H(U_1 | X_1 X_2, Z) \\ &\geq H(U_1 | X_2, Y, Z) - H(U_1 | X_1 X_2, Y, Z) \\ &= I(X_1; U_1 | X_2, Y, Z), \end{aligned}$$

which means that  $U_1$  is in  $\mathcal{A}(R_1)$ . Hence,  $\mathcal{A}^*(R_1) \subseteq \mathcal{A}(R_1)$ . This implies that

$$\begin{aligned} E_{SHA}(R_1) &\triangleq \max_{U_1 \in \mathcal{A}(R_1)} \min (\rho_1^*(U_1), \rho_2^*(U_1)) \\ &\geq \max_{U_1 \in \mathcal{A}^*(R_1)} \min (\rho_1^*(U_1), \rho_2^*(U_1)). \end{aligned} \tag{8}$$

Now the objective of the optimization problem in the definition of  $\rho_1^*(U_1)$  can be lower bounded as

$$\begin{aligned} D(P_{\tilde{U}_1 \tilde{X}_1 \tilde{X}_2 \tilde{Y} \tilde{Z}} \| P_{U_1 | X_1} P_{X_1 X_2 | Z} P_{Y | Z} P_Z) &\geq D(P_{\tilde{U}_1 \tilde{X}_2 \tilde{Y} \tilde{Z}} \| P_{U_1 X_2 | Z} P_{Y | Z} P_Z) \\ &= D(P_{U_1 X_2 Y Z} \| P_{U_1 X_2 | Z} P_{Y | Z} P_Z) \\ &= I(Y; U_1, X_2 | Z). \end{aligned}$$

The lower bound is achieved by the distribution  $P_{U_1 X_2 Y Z} P_{X_1 | U_1 X_2 Z}$  in  $\mathcal{B}(U_1)$ . Therefore,

$$\rho_1^*(U_1) = I(Y; U_1, X_2 | Z).$$

Similarly, we can lower bound the optimization problem in the definition of  $\rho_2(U_1)$  as

$$\begin{aligned} D(P_{\tilde{U}_1 \tilde{X}_1 \tilde{X}_2 \tilde{Y} \tilde{Z}} \| P_{U_1 | X_1} P_{X_1 X_2 | Z} P_{Y | Z} P_Z) &\geq D(P_{\tilde{X}_2 \tilde{Y} \tilde{Z}} \| P_{X_2 | Z} P_{Y | Z} P_Z) \\ &= D(P_{X_2 Y Z} \| P_{X_2 | Z} P_{Y | Z} P_Z) \\ &= I(Y; X_2 | Z), \end{aligned}$$

and the lower bound is achieved by the distribution  $P_{X_2 Y Z} P_{U_1 X_1 | X_2 Z}$  in  $\mathcal{C}(U_1)$ . Therefore,

$$\rho_2(U_1) = [R_1 - I(X_1; U_1 | X_2, Y, Z)]^+ + I(Y; X_2 | Z).$$

Consider any  $U_1$  in  $\mathcal{A}^*(R_1)$ . If  $R_1 \geq I(X_1; U_1)$ , then

$$\begin{aligned} \min (\rho_1^*(U_1), \rho_2^*(U_1)) &= \rho_1^*(U_1) \\ &= I(Y; U_1, X_2|Z). \end{aligned} \quad (9)$$

And if  $I(X_1; U_1) > R_1 \geq I(X_1; U_1|X_2, Z)$ , then

$$\begin{aligned} \min (\rho_1^*(U_1), \rho_2^*(U_1)) &= \min (I(Y; U_1, X_2|Z), R_1 - I(X_1; U_1|X_2, Y, Z) + I(Y; X_2|Z)) \\ &\geq \min (I(Y; U_1, X_2|Z), I(X_1; U_1|X_2, Z) - I(X_1; U_1|X_2, Y, Z) + I(Y; X_2|Z)) \\ &= \min (I(Y; U_1, X_2|Z), I(Y; U_1|X_2, Z) + I(Y; X_2|Z)) \\ &= \min (I(Y; U_1, X_2|Z), I(Y; U_1, X_2|Z)) \\ &= I(Y; U_1, X_2|Z). \end{aligned} \quad (10)$$

Now (8) through (10) imply

$$\begin{aligned} E_{SHA}(R_1) &\geq \max_{U_1 \in \mathcal{A}^*(R_1)} I(Y; U_1, X_2|Z) \\ &= E_{QBT}(R_1). \end{aligned}$$

Theorem 5 is thus proved.  $\square$

## 6 Gel'fand and Pinsker Hypothesis Testing against Independence

We now consider another special case, which we call the Gel'fand and Pinsker hypothesis testing against independence problem, because it is related to the source coding problem studied by Gel'fand and Pinsker [22].

Suppose that  $X_{L+1}$  and  $Z$  are deterministic and suppose there exists a function of  $X_1, \dots, X_L$ , say  $X$ , such that under  $H_0$ ,

(C5)  $X_1, \dots, X_L, Y$  are conditionally independent given  $X$ , and

(C6) for any finite-alphabet random variable  $U$  such that  $Y \leftrightarrow X \leftrightarrow U$  and  $Y \leftrightarrow U \leftrightarrow X$ , we have  $H(X|U) = 0$ .

Conditions (C5) and (C6) imply that under  $H_0$ ,  $X$  is a minimal sufficient statistic for  $Y$  given  $\mathbf{X}$  such that  $X_1, \dots, X_L, Y$  are conditionally independent given  $X$ . We shall characterize the centralized rate region, the set of rate vectors that achieve the centralized type 2 error exponent  $I(\mathbf{X}; Y) = I(X; Y)$ . More precisely, we shall characterize the set

$$\{\mathbf{R} : (\mathbf{R}, I(X; Y)) \in \mathcal{R}^{CI}\},$$

denoted by  $\mathcal{R}^{CI}(I(X; Y))$ . We define  $\mathcal{R}_i^{CI}(I(X; Y))$  and  $\overline{\mathcal{R}_o^{CI}}(I(X; Y))$  similarly. We need the following lemma.

**Lemma 2.** *Condition (C6) is equivalent to*

(C7) *For any positive  $\epsilon$ , there exists a positive  $\delta$  such that for all finite-alphabet random variables  $U$  such that  $Y \leftrightarrow X \leftrightarrow U$  and  $I(X; Y|U) \leq \delta$ , we have  $H(X|U) \leq \epsilon$ .*

The proof of Lemma 2 is presented in Appendix D. Let us define a function

$$\phi(\delta) \triangleq \inf \left\{ \epsilon : \text{for all finite-alphabet } U \text{ such that } Y \leftrightarrow X \leftrightarrow U \text{ and } I(X; Y|U) \leq \delta, \text{ we have } H(X|U) \leq \epsilon \right\}.$$

It is clear that  $\phi$  is continuous at zero with the value  $\phi(0) = 0$ . We have the following theorem.

**Theorem 6.** *For this problem, the centralized rate region*

$$\mathcal{R}^{CI}(I(X; Y)) = \mathcal{R}_i^{CI}(I(X; Y)) = \overline{\mathcal{R}_o^{CI}}(I(X; Y)).$$

*Proof.* It suffices to show that

$$\overline{\mathcal{R}_o^{CI}}(I(X; Y)) \subseteq \mathcal{R}_i^{CI}(I(X; Y)).$$

Consider any  $\mathbf{R}$  in  $\overline{\mathcal{R}_o^{CI}}(I(X; Y))$ , any positive  $\delta$ , and  $X$  defined as above. Then there exists  $\lambda_o = (\mathbf{U}, W, T)$  in  $\Lambda_o$  such that  $(R_1 + \delta, \dots, R_L + \delta, I(X; Y) - \delta)$  is in  $\mathcal{R}_o^{CI}(X, \lambda_o)$ , i.e.,

$$\sum_{l \in S} (R_l + \delta) \geq I(X; \mathbf{U}_S | \mathbf{U}_{S^c}, T) + \sum_{l \in S} I(X_l; U_l | X, W, T) \text{ for all } S \subseteq \mathcal{L}, \text{ and} \quad (11)$$

$$I(X; Y) - \delta \leq I(Y; \mathbf{U} | T). \quad (12)$$

We have the Markov chain

$$Y \leftrightarrow X \leftrightarrow (\mathbf{U}, T),$$

which implies

$$\begin{aligned} I(X; Y | \mathbf{U}, T) &= H(Y | \mathbf{U}, T) - H(Y | X, \mathbf{U}, T) \\ &= H(Y | \mathbf{U}, T) - H(Y | X) \\ &= I(X; Y) - I(Y; \mathbf{U} | T) \\ &\leq \delta, \end{aligned}$$

where the last inequality follows from (12). Therefore, by the definition of  $\phi$  function

$$H(X | \mathbf{U}, T) \leq \phi(\delta). \quad (13)$$

Now

$$\begin{aligned} I(X; \mathbf{U}_S | \mathbf{U}_{S^c}, T) &= H(X | \mathbf{U}_{S^c}, T) - H(X | \mathbf{U}, T) \\ &\geq H(X | \mathbf{U}_{S^c}, W, T) - \phi(\delta) \\ &\geq I(X; \mathbf{U}_S | \mathbf{U}_{S^c}, W, T) - \phi(\delta), \end{aligned} \quad (14)$$

where (14) follows from (13) and the fact that conditioning reduces entropy. This together with (11) implies

$$\begin{aligned} \sum_{l \in S} (R_l + \delta + \phi(\delta)) &\geq I(X; \mathbf{U}_S | \mathbf{U}_{S^c}, W, T) + \sum_{l \in S} I(X_l; U_l | X, W, T) \\ &= I(X; \mathbf{U}_S | \mathbf{U}_{S^c}, W, T) + I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c}, X, W, T) \\ &= I(X, \mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c}, W, T) \\ &\geq I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c}, W, T). \end{aligned}$$

Again since conditioning reduces entropy and  $Y$  is independent of  $(W, T)$ , we obtain from (12) that

$$\begin{aligned} I(X; Y) - \delta &\leq I(Y; \mathbf{U} | T) \\ &= H(Y | T) - H(Y | \mathbf{U}, T) \\ &\leq H(Y | W, T) - H(Y | \mathbf{U}, W, T) \\ &= I(Y; \mathbf{U} | W, T). \end{aligned}$$

Define  $\tilde{T} = (W, T)$ . It is then clear that  $\lambda_i = (\mathbf{U}, \tilde{T})$  is in  $\Lambda_i$ ,

$$\sum_{l \in S} (R_l + \delta + \phi(\delta)) \geq I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c}, \tilde{T}) \text{ for all } S \subseteq \mathcal{L}, \text{ and}$$

$$I(X; Y) - \delta \leq I(Y; \mathbf{U} | \tilde{T}).$$

Hence,  $(R_1 + \delta + \phi(\delta), \dots, R_L + \delta + \phi(\delta), I(X; Y) - \delta)$  is in  $\mathcal{R}_i^{CI}(\lambda_i)$ , which implies that  $(\mathbf{R}, I(X; Y))$  is in  $\mathcal{R}_i^{CI}$  because  $\mathcal{R}_i^{CI}$  is closed from Lemma 1(b). Therefore,  $\mathbf{R}$  is in  $\mathcal{R}_i^{CI}(I(X; Y))$ .  $\square$

## 7 Gaussian Many-Help-One Hypothesis Testing against Independence

We now turn to a continuous example of the problem studied in Section 4. This problem is related to the quadratic Gaussian many-help-one source coding problem [18, 23, 24]. We first obtain an outer bound similar to the one in Theorem 2 and then show that it is achieved by the Quantize-Bin-Test scheme.

Let  $(X, Y, X_1, \dots, X_L)$  be a zero-mean Gaussian random vector such that

$$X_l = X + N_l$$

for each  $l$  in  $\mathcal{L}$ .  $X$  and  $Y$  are correlated under the null hypothesis  $H_0$  and are independent under the alternate hypothesis  $H_1$ , i.e.,

$$H_0 : Y = X + N$$

$$H_1 : Y \perp\!\!\!\perp X.$$

We assume that  $X, N, N_1, N_2, \dots, N_L$  are mutually independent, and that  $\sigma_N^2$  and  $\sigma_{N_l}^2$  are positive. The setup of the problem is shown in Fig. 4. Unlike the previous problem, we now allow  $X$  to be observed by an encoder, which sends a message to the detector at a finite rate  $R$ . We use  $f^{(n)}$  to denote the corresponding encoding function. In order to be consistent with the source coding terminology, we call this the main encoder. The encoder observing  $X_l$  is now called helper  $l$ . We assume that  $X_{L+1}$  and  $Z$  are deterministic. The rest of the problem formulation is the same as the one in Section 3.1. Let  $\mathcal{R}^{MHO}$  be the rate-exponent region of this problem. We need the entropy characterization of  $\mathcal{R}^{MHO}$ . For that, define

$$\mathcal{R}_*^{MHO} \triangleq \bigcup_n \bigcup_{f^{(n)}, (f_l^{(n)})_{l \in \mathcal{L}}} \mathcal{R}_*^{MHO} \left( n, (f_l^{(n)})_{l \in \mathcal{L}} \right),$$

where

$$\mathcal{R}_*^{MHO} \left( n, (f_l^{(n)})_{l \in \mathcal{L}} \right) \triangleq \left\{ (R, \mathbf{R}, E) : R \geq \frac{1}{n} \log |f^{(n)}(X^n)|, \right.$$

$$R_l \geq \frac{1}{n} \log |f_l^{(n)}(X_l^n)| \text{ for all } l \text{ in } \mathcal{L}, \text{ and}$$

$$\left. E \leq \frac{1}{n} I \left( Y^n; f^{(n)}(X^n), (f_l^{(n)}(X_l^n))_{l \in \mathcal{L}} \right) \right\}.$$

**Corollary 2.**  $\mathcal{R}^{MHO} = \overline{\mathcal{R}_*^{MHO}}$ .

The proof of this result is almost identical to that of Proposition 1. Define the set

$$\tilde{\mathcal{R}}^{MHO} \triangleq \left\{ (R, R_1, \dots, R_L, E) : \text{there exists } (r_1, \dots, r_L) \in \mathbb{R}_+^L \text{ such that} \right.$$

$$R_l \geq r_l \text{ for all } l \text{ in } \mathcal{L}, \text{ and}$$

$$\left. R + \sum_{l \in S} R_l \geq \frac{1}{2} \log^+ \left[ \frac{1}{D} \left( \frac{1}{\sigma_X^2} + \sum_{l \in S^c} \frac{1 - 2^{-2r_l}}{\sigma_{N_l}^2} \right)^{-1} \right] + \sum_{l \in S} r_l \text{ for all } S \subseteq \mathcal{L} \right\},$$

where

$$D = (\sigma_X^2 + \sigma_N^2)2^{-2E} - \sigma_N^2.$$

**Theorem 7.** *The rate-exponent region of this problem*

$$\mathcal{R}^{MHO} = \tilde{\mathcal{R}}^{MHO}.$$

*Proof.* The proof of inclusion  $\mathcal{R}^{MHO} \subseteq \tilde{\mathcal{R}}^{MHO}$  is similar to the converse proof of the Gaussian many-help-one source coding problem by Oohama [23] and Prabhakaran *et al.* [24] (see also [16]). Their proofs continue to work if we replace the original mean square error distortion constraint with the mutual information constraint that we have here. It is noteworthy though that Wang *et al.*'s [33] approach does not work here because it relies on the distortion constraint.

We start with the continuous extension of Theorem 2. Let  $\Lambda_o$  be the set of random variables  $\lambda_o = (U, \mathbf{U}, W, T)$  such that each take values in a finite-dimensional Euclidean space and collectively they satisfy

(C8)  $(W, T)$  is independent of  $(X, \mathbf{X}, Y)$ ,

(C9)  $U \leftrightarrow (X, W, T) \leftrightarrow (\mathbf{U}, \mathbf{X}, Y)$ ,

(C10)  $U_l \leftrightarrow (X_l, W, T) \leftrightarrow (U, \mathbf{U}_{l^c}, X, \mathbf{X}_{l^c}, Y)$  for all  $l$  in  $\mathcal{L}$ , and

(C11) the conditional distribution of  $U_l$  given  $(W, T)$  is discrete for each  $l$ .

Define the set

$$\mathcal{R}_o^{MHO}(\lambda_o) \triangleq \left\{ (R, \mathbf{R}, E) : R_l \geq I(X_l; U_l | X, W, T) \text{ for all } l \text{ in } \mathcal{L}, \right. \quad (15)$$

$$\left. R + \sum_{l \in S} R_l \geq I(X; U, \mathbf{U}_S | \mathbf{U}_{S^c}, T) + \sum_{l \in S} I(X_l; U_l | X, W, T) \text{ for all } S \subseteq \mathcal{L}, \text{ and} \right. \quad (16)$$

$$\left. E \leq I(Y; U, \mathbf{U} | T) \right\}. \quad (17)$$

Finally, let

$$\mathcal{R}_o^{MHO} \triangleq \bigcup_{\lambda_o \in \Lambda_o} \mathcal{R}_o^{CI}(\lambda_o).$$

We have the following lemma.

**Lemma 3.**  $\mathcal{R}_*^{MHO} \subseteq \mathcal{R}_o^{MHO}$ .

The inequalities (16) and (17) can be established as in the proof of Theorem 2. In particular, we obtain (16) by considering only those constraints on the sum of rate combinations that include  $R$ . The inequality (15) is not present in Theorem 2. However, it can be derived easily. We need the following lemma.

**Lemma 4.** [16, Lemma 9] *If  $\lambda_o$  is in  $\Lambda_o$ , then for all  $S \subseteq \mathcal{L}$ ,*

$$2^{2I(X; \mathbf{U}_S | W, T)} \leq 1 + \sum_{l \in S} \frac{1 - 2^{-2I(X_l; U_l | X, W, T)}}{\sigma_{N_l}^2 / \sigma_X^2}.$$

Consider any  $(R, \mathbf{R}, E)$  in  $\mathcal{R}_o^{MHO}$ . Then there exists  $\lambda_o$  in  $\Lambda_o$  such that for all  $S \subseteq \mathcal{L}$ ,

$$\begin{aligned} R + \sum_{l \in S} R_l &\geq I(X; U, \mathbf{U}_S | \mathbf{U}_{S^c}, T) + \sum_{l \in S} I(X_l; U_l | X, W, T) \\ &= I(X; U, \mathbf{U} | T) - I(X; \mathbf{U}_{S^c} | T) + \sum_{l \in S} I(X_l; U_l | X, W, T), \end{aligned} \quad (18)$$

and

$$E \leq I(Y; U, \mathbf{U}|T). \quad (19)$$

We can lower bound the first term in (18) by applying the entropy power inequality [34] and obtain

$$\begin{aligned} 2^{2h(Y|U, \mathbf{U}, T)} &= 2^{2h(X+N|U, \mathbf{U}, T)} \\ &\geq 2^{2h(X|U, \mathbf{U}, T)} + 2^{2h(N)} \\ &= 2^{2h(X|U, \mathbf{U}, T)} + 2\pi e \sigma_N^2, \end{aligned}$$

which simplifies to

$$h(Y|U, \mathbf{U}, T) \geq \frac{1}{2} \log \left( 2^{2h(X|U, \mathbf{U}, T)} + 2\pi e \sigma_N^2 \right). \quad (20)$$

Now (19) and (20) together imply

$$I(X; U, \mathbf{U}|T) \geq \frac{1}{2} \log \frac{\sigma_X^2}{(\sigma_X^2 + \sigma_N^2)2^{-2E} - \sigma_N^2}. \quad (21)$$

We next upper bound the second term in (18). Since conditioning reduces entropy and  $X$  is independent of  $(W, T)$ , we have

$$\begin{aligned} I(X; \mathbf{U}_{S^c}|T) &= h(X|T) - h(X|\mathbf{U}_{S^c}, T) \\ &\leq h(X|W, T) - h(X|\mathbf{U}_{S^c}, W, T) \\ &= I(X; \mathbf{U}_{S^c}|W, T). \end{aligned} \quad (22)$$

Define

$$r_l \triangleq I(X_l; U_l|X, W, T).$$

Then we have from (18), (21), (22), and Lemma 4 that

$$R + \sum_{l \in S} R_l \geq \frac{1}{2} \log^+ \left[ \frac{1}{((\sigma_X^2 + \sigma_N^2)2^{-2E} - \sigma_N^2)} \left( \frac{1}{\sigma_X^2} + \sum_{l \in S^c} \frac{1 - 2^{-2r_l}}{\sigma_{N_l}^2} \right)^{-1} \right] + \sum_{l \in S} r_l.$$

On applying Lemma 3 and Corollary 2, we obtain  $\mathcal{R}^{MHO} \subseteq \tilde{\mathcal{R}}^{MHO}$ .

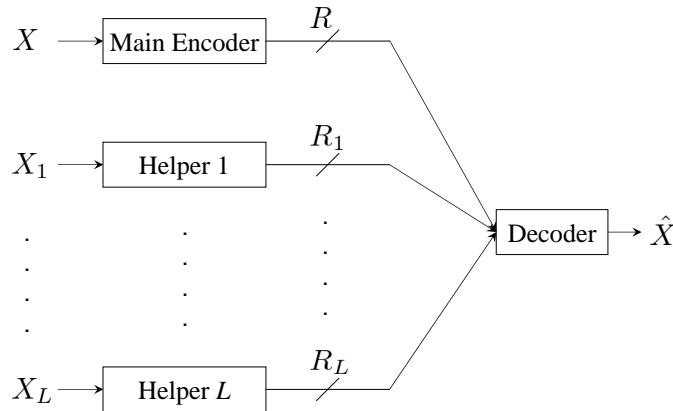


Figure 6: Gaussian many-help-one source coding problem

We use the Quantize-Bin-Test scheme to prove the reverse inclusion. Consider  $(R, \mathbf{R}, E)$  in  $\tilde{\mathcal{R}}^{MHO}$ . Then there exists  $\mathbf{r} \in \mathbb{R}_+^L$  such that

$$R_l \geq r_l \text{ for all } l \text{ in } \mathcal{L}, \text{ and}$$

$$R + \sum_{l \in S} R_l \geq \frac{1}{2} \log^+ \left[ \frac{1}{D} \left( \frac{1}{\sigma_X^2} + \sum_{l \in S^c} \frac{1 - 2^{-2r_l}}{\sigma_{N_l}^2} \right)^{-1} \right] + \sum_{l \in S} r_l \text{ for all } S \subseteq \mathcal{L}.$$

We therefore have from Oohama's result [23] that  $(R, \mathbf{R}, D)$  is achievable for the quadratic Gaussian many-help-one source coding problem, the setup of which is shown in Fig. 6. In this problem, the main encoder and helpers operate as before. The decoder however uses all available information to estimate  $X$  such that the mean square error of the estimate is no more than a fixed positive number  $D$ . Since  $(R, \mathbf{R}, D)$  is achievable, it follows by Oohama's achievability proof that for any positive  $\delta$  and sufficiently large  $n$ , there exists quantize and bin encoders  $f^{(n)}, f_1^{(n)}, \dots, f_L^{(n)}$ , and a decoder  $\psi^{(n)}$  such that

$$R + \delta \geq \frac{1}{n} \log \left| f^{(n)}(X^n) \right|, \quad (23)$$

$$R_l + \delta \geq \frac{1}{n} \log \left| f_l^{(n)}(X_l^n) \right| \text{ for all } l \text{ in } \mathcal{L}, \text{ and} \quad (24)$$

$$D + \delta \geq \frac{1}{n} \sum_{i=1}^n E \left[ \left( X^n(i) - \hat{X}^n(i) \right)^2 \right], \quad (25)$$

where

$$\hat{X}^n = \psi^{(n)} \left( f^{(n)}(X^n), \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}} \right).$$

For each  $i$ , we have

$$\begin{aligned} E \left[ \left( Y^n(i) - \hat{X}^n(i) \right)^2 \right] &= E \left[ \left( Y^n(i) - X^n(i) + X^n(i) - \hat{X}^n(i) \right)^2 \right] \\ &= E \left[ \left( N^n(i) + X^n(i) - \hat{X}^n(i) \right)^2 \right] \\ &= \sigma_N^2 + E \left[ \left( X^n(i) - \hat{X}^n(i) \right)^2 \right], \end{aligned}$$

where the last equality follows because

$$Y^n(i) \leftrightarrow X^n(i) \leftrightarrow \hat{X}^n(i).$$

By averaging over time, we obtain

$$\begin{aligned} \frac{1}{n} \sum_{i=1}^n E \left[ \left( Y^n(i) - \hat{X}^n(i) \right)^2 \right] &= \sigma_N^2 + \frac{1}{n} \sum_{i=1}^n E \left[ \left( X^n(i) - \hat{X}^n(i) \right)^2 \right] \\ &\leq \sigma_N^2 + D + \delta, \end{aligned}$$

where the last inequality follows from (25). Therefore, the code achieves a distortion  $\sigma_N^2 + D + \delta$  in  $Y$ . Hence,

$$\frac{1}{n} I \left( Y^n; f^{(n)}(X^n), \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}} \right)$$

must be no less than the rate-distortion function of  $Y$  at a distortion  $\sigma_N^2 + D + \delta$ , i.e.,

$$\begin{aligned} \frac{1}{n} I \left( Y^n; f^{(n)}(X^n), \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}} \right) &\geq \frac{1}{2} \log \frac{\sigma_X^2 + \sigma_N^2}{\sigma_N^2 + D + \delta} \\ &= \frac{1}{2} \log \frac{\sigma_X^2 + \sigma_N^2}{(\sigma_X^2 + \sigma_N^2) 2^{-2E} + \delta} \\ &\geq \frac{1}{2} \log \frac{\sigma_X^2 + \sigma_N^2}{(\sigma_X^2 + \sigma_N^2) 2^{-2(E-\bar{\delta})}} \end{aligned} \quad (26)$$

$$= E - \bar{\delta}, \quad (27)$$

where (26) follows for a positive  $\bar{\delta}$  such that  $\bar{\delta} \rightarrow 0$  as  $\delta \rightarrow 0$ . We now have from (23), (24), and (27) that  $(R, \mathbf{R}, E)$  is in  $\overline{\mathcal{R}_*^{MHO}}$ . Hence by Corollary 2,  $\tilde{\mathcal{R}}^{MHO} \subseteq \mathcal{R}^{MHO}$ .  $\square$

## 7.1 Special Cases

Consider the following special cases. We continue to use the terminology from the source coding literature.

1. *Gaussian CEO hypothesis testing against independence:* When  $R = 0$ , the problem reduces to the Gaussian CEO hypothesis testing against independence problem. Let  $\mathcal{R}^{CEO}$  be the rate-exponent region of this problem. Define the set

$$\tilde{\mathcal{R}}^{CEO} \triangleq \left\{ (R_1, \dots, R_L, E) : \text{there exists } \mathbf{r} \in \mathbb{R}_+^L \text{ such that} \right. \\ \left. \sum_{l \in S} R_l \geq \frac{1}{2} \log^+ \left[ \frac{1}{D} \left( \frac{1}{\sigma_X^2} + \sum_{l \in S^c} \frac{1 - 2^{-2r_l}}{\sigma_{N_l}^2} \right)^{-1} \right] + \sum_{l \in S} r_l \text{ for all } S \subseteq \mathcal{L} \right\}.$$

We immediately have the following corollary as a consequence of Theorem 7.

**Corollary 3.**  $\mathcal{R}^{CEO} = \tilde{\mathcal{R}}^{CEO}$ .

2. *Gaussian one-helper hypothesis testing against independence:* When  $L = 1$ , the problem reduces to the Gaussian one-helper hypothesis testing against independence problem. Let  $\mathcal{R}^{OH}$  be the rate-exponent region of this problem. Define the sets

$$\tilde{\mathcal{R}}^{OH} \triangleq \left\{ (R, R_1, E) : \text{there exists } r_1 \in \mathbb{R}_+ \text{ such that} \right. \\ R_1 \geq r_1, \\ R + R_1 \geq \frac{1}{2} \log^+ \left[ \frac{\sigma_X^2}{D} \right] + r_1, \text{ and} \\ \left. R \geq \frac{1}{2} \log^+ \left[ \frac{1}{D} \left( \frac{1}{\sigma_X^2} + \frac{1 - 2^{-2r_1}}{\sigma_{N_1}^2} \right)^{-1} \right] \right\},$$

and

$$\bar{\mathcal{R}}^{OH} \triangleq \left\{ (R, R_1, E) : R \geq \frac{1}{2} \log^+ \left[ \frac{\sigma_X^2}{D} (1 - \rho^2 + \rho^2 2^{-2R_1}) \right] \right\},$$

where

$$\rho^2 = \frac{\sigma_X^2}{\sigma_X^2 + \sigma_{N_1}^2}.$$

**Corollary 4.**  $\mathcal{R}^{OH} = \tilde{\mathcal{R}}^{OH} = \bar{\mathcal{R}}^{OH}$ .

*Proof.* The first equality follows from Theorem 7. Consider any  $(R, R_1, E)$  in  $\tilde{\mathcal{R}}^{OH}$ . It must satisfy

$$R \geq \min_{0 \leq r_1 \leq R_1} \max \left\{ \frac{1}{2} \log^+ \left[ \frac{1}{D} \left( \frac{1}{\sigma_X^2} + \frac{1 - 2^{-2r_1}}{\sigma_{N_1}^2} \right)^{-1} \right], \frac{1}{2} \log^+ \left[ \frac{\sigma_X^2}{D} \right] + r_1 - R_1 \right\} \\ = \frac{1}{2} \log^+ \left[ \frac{\sigma_X^2}{D} (1 - \rho^2 + \rho^2 2^{-2R_1}) \right],$$

where the equality is achieved by

$$r_1 = R_1 + \frac{1}{2} \log (1 - \rho^2 + \rho^2 2^{-2R_1}). \quad (28)$$

We therefore have that  $(R, R_1, E)$  is in  $\bar{\mathcal{R}}^{OH}$ , and hence  $\tilde{\mathcal{R}}^{OH} \subseteq \bar{\mathcal{R}}^{OH}$ . The proof of the reverse containment follows by noticing that for any  $(R, R_1, E)$  in  $\bar{\mathcal{R}}^{OH}$ , there exists  $r_1$  as in (28) such that all inequalities in the definition of  $\tilde{\mathcal{R}}^{OH}$  are satisfied.  $\square$

## 8 A General Outer Bound

We return to the general problem formulated in Section 3. The problem remains open till date. Several inner bounds are known for  $L = 1$  [4, 5, 6, 7]. But even for  $L = 1$ , there is no nontrivial outer bound with which to compare the inner bounds. We give an outer bound for a class of instances of the general problem.

Consider the class of instances such that  $P_{\mathbf{X}} = Q_{\mathbf{X}}$ , i.e., the marginal distributions of  $\mathbf{X}$  are the same under both hypotheses. Stein's lemma [34] asserts that the centralized type 2 error exponent for this class of problems is

$$E_C \triangleq D(P_{\mathbf{X}Y} \| Q_{\mathbf{X}Y}),$$

which is achieved when  $\mathbf{X}$  and  $Y$  both are available at the detector. Let

$$\mathcal{R}_C \triangleq \{(\mathbf{R}, E) : E \leq E_C\}.$$

We have the following trivial centralized outer bound.

**Lemma 5.**  $\mathcal{R} \subseteq \mathcal{R}_C$ .

Let  $\Xi$  be the set of random variables  $Z$  such that there exists two joint distributions  $P_{\mathbf{X}YZ}$  and  $Q_{\mathbf{X}YZ}$  satisfying

$$(C12) \quad \sum_Z P_{\mathbf{X}YZ} = P_{\mathbf{X}Y}, \text{ the distribution under } H_0,$$

$$(C13) \quad \sum_Z Q_{\mathbf{X}YZ} = Q_{\mathbf{X}Y}, \text{ the distribution under } H_1,$$

$$(C14) \quad Q_{\mathbf{X}YZ} = Q_{\mathbf{X}|Z} Q_{Y|Z} Q_Z, \text{ i.e., } \mathbf{X} \text{ and } Y \text{ are conditionally independent given } Z \text{ under the } Q \text{ distribution, and}$$

$$(C15) \quad P_{\mathbf{X}Z} = Q_{\mathbf{X}Z}, \text{ i.e., the joint distributions of } (\mathbf{X}, Z) \text{ are the same under both distributions.}$$

Note that the joint distributions of  $(Y, Z)$  need not be the same under the two distributions. If  $P_{\mathbf{X}YZ}$  and  $Q_{\mathbf{X}YZ}$  are the joint distributions of  $\mathbf{X}$ ,  $Y$ , and  $Z$  under  $H_0$  and  $H_1$ , respectively and  $Z$  is available to the detector, then the problem can be related to the  $L$ -encoder hypothesis testing against conditional independence. Now  $Z$  is not present in the original problem, but we can augment the sample space by introducing  $Z$  and supplying it to the decoder. The outer bound for this new problem is then an outer bound for the original problem. Moreover, we can then optimize over  $Z$  to obtain the best possible bound.

Let  $\chi$  and  $\Lambda_o$  be defined as in Section 4.2 with  $X_{L+1}$  restricted to be deterministic. If  $\Xi$  is nonempty, then for any  $(Z, X, \lambda_o)$  in  $\Xi \times \chi \times \lambda_o$ , define the set

$$\mathcal{R}_o(Z, X, \lambda_o) \triangleq \left\{ (\mathbf{R}, E) : \sum_{l \in S} R_l \geq I(X; \mathbf{U}_S | \mathbf{U}_{S^c}, Z, T) + \sum_{l \in S} I(X_l; U_l | X, W, Z, T) \text{ for all } S \subseteq \mathcal{L}, \text{ and } \right. \\ \left. E \leq I(Y; \mathbf{U} | Z, T) + D(P_{Y|Z} \| Q_{Y|Z} | Z) \right\}.$$

Finally, let

$$\mathcal{R}_o \triangleq \begin{cases} \bigcap_{Z \in \Xi} \bigcap_{X \in \chi} \bigcup_{\lambda_o \in \Lambda_o} \mathcal{R}_o(Z, X, \lambda_o) & \text{if } \Xi \text{ is nonempty} \\ \mathbb{R}_+^{L+1} & \text{otherwise.} \end{cases}$$

We have the following outer bound to the rate-exponent region of this class of problems.

**Theorem 8.**  $\mathcal{R} \subseteq \overline{\mathcal{R}_o} \cap \mathcal{R}_C$ .

*Proof.* In light of Proposition 1 and Lemma 5, it suffices to show that

$$\mathcal{R}_* \subseteq \mathcal{R}_o.$$

Consider  $(\mathbf{R}, E)$  in  $\mathcal{R}_*$ . Then there exists a block length  $n$  and encoders  $f_l^{(n)}$  such that

$$R_l \geq \frac{1}{n} \log \left| f_l^{(n)}(X_l^n) \right| \text{ for all } l \text{ in } \mathcal{L}, \text{ and} \quad (29)$$

$$E \leq \frac{1}{n} D \left( P_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}} Y^n} \parallel Q_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}} Y^n} \right). \quad (30)$$

Consider any  $Z$  in  $\Xi$ . Then

$$\begin{aligned} & D \left( P_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}} Y^n} \parallel Q_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}} Y^n} \right) \\ & \leq D \left( P_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}} Y^n Z^n} \parallel Q_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}} Y^n Z^n} \right) \\ & = D \left( P_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}} Y^n | Z^n} \parallel Q_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}} Y^n | Z^n} \right) \\ & = D \left( P_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}} Y^n | Z^n} \parallel P_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}} | Z^n} Q_{Y^n | Z^n} \right) \\ & = D \left( P_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}} Y^n | Z^n} \parallel P_{(f_l^{(n)}(X_l^n))_{l \in \mathcal{L}} | Z^n} P_{Y^n | Z^n} \right) + D \left( P_{Y^n | Z^n} \parallel Q_{Y^n | Z^n} \right) \\ & = I \left( \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}} ; Y^n | Z^n \right) + n D \left( P_{Y | Z} \parallel Q_{Y | Z} \right), \end{aligned}$$

which together with (30) implies

$$E \leq \frac{1}{n} I \left( \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}} ; Y^n | Z^n \right) + D \left( P_{Y | Z} \parallel Q_{Y | Z} \right). \quad (31)$$

It now follows from (29), (31), and Corollary 1 that  $(\mathbf{R}, (E - D(P_{Y|Z} \parallel Q_{Y|Z})))^+$  is in  $\mathcal{R}_*^{CI}$ . Therefore from Theorem 2, it must also be in  $\mathcal{R}_o^{CI}$ . Hence for any  $X$  in  $\chi$ , there exists  $\lambda_o$  in  $\Lambda_o$  such that  $(\mathbf{R}, (E - D(P_{Y|Z} \parallel Q_{Y|Z})))^+$  is in  $\mathcal{R}_o^{CI}(X, \lambda_o)$ , i.e.,

$$\begin{aligned} \sum_{l \in S} R_l & \geq I(X; \mathbf{U}_S | \mathbf{U}_{S^c}, Z, T) + \sum_{l \in S} I(X_l; U_l | X, W, Z, T) \text{ for all } S \subseteq \mathcal{L}, \text{ and} \\ (E - D(P_{Y|Z} \parallel Q_{Y|Z}))^+ & \leq I(Y; \mathbf{U} | Z, T). \end{aligned}$$

This means that  $(\mathbf{R}, E)$  is in  $\mathcal{R}_o(Z, X, \lambda_o)$ , and hence  $\mathcal{R}_* \subseteq \mathcal{R}_o$ . □

Although the outer bound above is not computable in general, it simplifies to the following computable form for the special case in which  $L = 1$ . Let

$$\begin{aligned} \tilde{\mathcal{R}} & \triangleq \bigcap_{Z \in \Xi} \left\{ (R_1, E) : \text{there exists } U_1 \text{ such that} \right. \\ & \quad R_1 \geq I(X_1; U_1 | Z), \\ & \quad E \leq I(Y; U_1 | Z) + D(P_{Y|Z} \parallel Q_{Y|Z}), \\ & \quad |\mathcal{U}_1| \leq |\mathcal{X}_1| + 1, \text{ and} \\ & \quad \left. U_1 \leftrightarrow X_1 \leftrightarrow (Y, Z) \right\}. \end{aligned}$$

**Corollary 5.** For 1-encoder general hypothesis testing,  $\overline{\mathcal{R}_o} = \tilde{\mathcal{R}}$  and hence  $\mathcal{R} \subseteq \tilde{\mathcal{R}} \cap \mathcal{R}_C$ .

*Proof.* It suffices to show that  $\overline{\mathcal{R}_o} = \tilde{\mathcal{R}}$ . This immediately follows by noticing that given any  $Z$  in  $\Xi$ , the outer bound can be related to the rate-exponent region of the 1-encoder hypothesis testing against conditional independence problem. The result then follows from Theorem 3. □

It is easy to see that the outer bound is tight for the test against independence.

**Corollary 6.** (Test against independence, [5]) If  $Q_{X_1Y} = P_{X_1}P_Y$ , then

$$\mathcal{R} = \tilde{\mathcal{R}}.$$

*Proof.* This follows by choosing  $Z$  to be deterministic in the outer bound and then invoking the result of Ahlswede and Csiszár [5].  $\square$

*Remark 2:* The outer bound is not always better than the centralized outer bound. In particular, if

$$D(P_{Y|Z} \| Q_{Y|Z} | Z) \geq E_C$$

for all  $Z$  in  $\Xi$ , then the outer bound is no better than the centralized outer bound.

## 8.1 Gaussian Case

To illustrate this bound, let us consider a Gaussian example in which  $X_1$  and  $Y$  are zero-mean unit-variance jointly Gaussian sources with the correlation coefficients  $\rho_0$  and  $\rho_1$  under  $H_0$  and  $H_1$ , respectively, where  $\rho_0 \neq \rho_1$ ,  $\rho_0^2 < 1$ , and  $\rho_1^2 < 1$ . We can assume without loss of generality that  $0 \leq \rho_1 < 1$  because the case  $-1 < \rho_1 \leq 0$  can be handled by multiplying  $Y$  by  $-1$ . We use lowercase  $p$  and  $q$  to denote appropriate Gaussian densities under hypotheses  $H_0$  and  $H_1$ , respectively. Let  $\mathcal{R}^G$  be the rate-exponent region of this problem. We focus on the following three regions (Fig. 7) for which the outer bound is nontrivial.

$$\mathcal{D}_1 \triangleq \{(\rho_0, \rho_1) : 0 \leq \rho_1 < \rho_0 < 1\},$$

$$\mathcal{D}_2 \triangleq \{(\rho_0, \rho_1) : 0 \leq \rho_1 \text{ and } 2\rho_1 - 1 \leq \rho_0 < \rho_1\},$$

$$\mathcal{D}_3 \triangleq \left\{ (\rho_0, \rho_1) : -1 < \rho_0 \leq 2\rho_1 - 1 \text{ and } \frac{2(\log e)\rho_1}{1 - \rho_1} \leq \frac{1}{2} \log \left( \frac{1 - \rho_1^2}{1 - \rho_0^2} \right) - \frac{(\log e)\rho_1(\rho_0 - \rho_1)}{1 - \rho_1^2} \right\}.$$

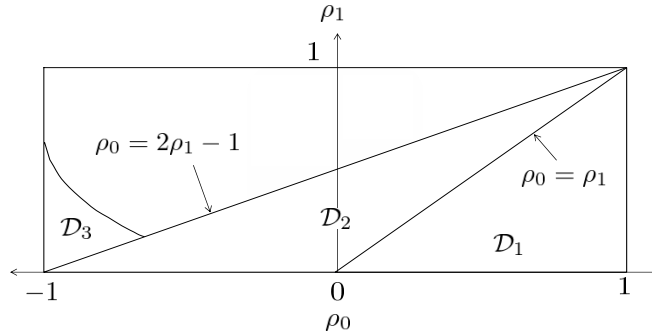


Figure 7: Regions of pair  $(\rho_0, \rho_1)$  for which the outer bound is nontrivial

### 8.1.1 Outer Bound

Let us define

$$\rho \triangleq \begin{cases} \frac{\rho_0 - \rho_1}{1 - \rho_1} & \text{if } (\rho_0, \rho_1) \text{ is in } \mathcal{D}_1 \cup \mathcal{D}_2 \\ \frac{\rho_0 + \rho_1}{1 - \rho_1} & \text{if } (\rho_0, \rho_1) \text{ is in } \mathcal{D}_3. \end{cases}$$

and

$$C \triangleq \begin{cases} 0 & \text{if } (\rho_0, \rho_1) \text{ is in } \mathcal{D}_1 \cup \mathcal{D}_2 \\ \frac{2(\log e)\rho_1}{1-\rho_1} & \text{if } (\rho_0, \rho_1) \text{ is in } \mathcal{D}_3. \end{cases}$$

The centralized type 2 error exponent is

$$\begin{aligned} E_C^G &\triangleq D(p_{X_1Y} \| q_{X_1Y}) \\ &= \frac{1}{2} \log \left( \frac{1-\rho_1^2}{1-\rho_0^2} \right) - \frac{(\log e)\rho_1(\rho_0 - \rho_1)}{1-\rho_1^2}. \end{aligned}$$

Define the sets

$$\mathcal{R}_o^G \triangleq \left\{ (R_1, E) : E \leq \frac{1}{2} \log \left( \frac{1}{1-\rho^2 + \rho^2 2^{-2R_1}} \right) + C \right\}$$

and

$$\mathcal{R}_C^G \triangleq \{ (R_1, E) : E \leq E_C^G \}.$$

We have the following outer bound.

**Theorem 9.** *If  $(\rho_0, \rho_1)$  is in  $\mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3$ , then*

$$\mathcal{R}^G \subseteq \mathcal{R}_o^G \cap \mathcal{R}_C^G.$$

*Proof.* The proof is in two steps: obtain a single letter outer bound similar to the one in Corollary 5 and then use it to obtain the desired outer bound. Consider  $(\rho_0, \rho_1)$  in  $\mathcal{D}_1$ . Let  $Z, Z', W$ , and  $V$  be standard normal random variables independent of each other.  $X_1$  and  $Y$  can be expressed as

$$\begin{aligned} X_1 &= \sqrt{\rho_1}Z + \sqrt{\rho_0 - \rho_1}Z' + \sqrt{1 - \rho_0}W \\ Y &= \sqrt{\rho_1}Z + \sqrt{\rho_0 - \rho_1}Z' + \sqrt{1 - \rho_0}V \end{aligned}$$

under  $H_0$  and as

$$\begin{aligned} X_1 &= \sqrt{\rho_1}Z + \sqrt{1 - \rho_1}W \\ Y &= \sqrt{\rho_1}Z + \sqrt{1 - \rho_1}V \end{aligned}$$

under  $H_1$ . It is easy to verify that conditions (C12) through (C15) are satisfied if we replace the distributions by the corresponding Gaussian densities. Therefore,  $Z$  is in  $\Xi$ . Define the set

$$\begin{aligned} \tilde{\mathcal{R}}^G &\triangleq \left\{ (R_1, E) : \text{there exists } U_1 \text{ such that} \right. \\ &\quad R_1 \geq I(X_1; U_1 | Z), \\ &\quad E \leq I(Y; U_1 | Z) + D(p_{Y|Z} \| q_{Y|Z} | Z), \text{ and} \\ &\quad \left. (Y, Z) \leftrightarrow X_1 \leftrightarrow U_1 \right\}. \end{aligned}$$

**Corollary 7.**  $\mathcal{R}^G \subseteq \overline{\tilde{\mathcal{R}}^G} \cap \mathcal{R}_C^G$ .

The proof is immediate as a continuous extension of Corollary 5. From Corollary 7, it suffices to show that

$$\tilde{\mathcal{R}}^G \subseteq \mathcal{R}_o^G.$$

Note first that

$$D(p_{Y|Z} \| q_{Y|Z} | Z) = 0$$

here because the joint densities of  $(Y, Z)$  are the same under both hypotheses. Consider any  $(R_1, E)$  in  $\tilde{\mathcal{R}}^G$ . Then there exists a random variable  $U_1$  such that  $(Y, Z) \leftrightarrow X_1 \leftrightarrow U_1$ ,

$$R_1 \geq I(X_1; U_1|Z), \text{ and} \quad (32)$$

$$E \leq I(Y; U_1|Z). \quad (33)$$

Since  $X_1, Y$ , and  $Z$  are jointly Gaussian under  $H_0$ , we can write that

$$Y = \rho X_1 + \sqrt{\rho_1}(1 - \rho)Z + B,$$

where  $B$  is a zero-mean Gaussian random variable with the variance

$$\sigma_{Y|X_1Z}^2 = (1 - \rho_1)(1 - \rho^2),$$

and is independent of  $X_1$  and  $Z$ . We now have

$$\begin{aligned} h(Y|U_1, Z) &= h(\rho X_1 + \sqrt{\rho_1}(1 - \rho)Z + B|U_1, Z) \\ &= h(\rho X_1 + B|U_1, Z) \\ &\geq \frac{1}{2} \log \left( 2^{2h(\rho X_1|U_1, Z)} + 2^{2h(B)} \right) \end{aligned} \quad (34)$$

$$\begin{aligned} &= \frac{1}{2} \log \left( \rho^2 2^{2h(X_1|U_1, Z)} + 2^{2h(B)} \right) \\ &= \frac{1}{2} \log \left( \rho^2 2^{2(h(X_1|Z) - I(X_1; U_1|Z))} + 2^{2h(B)} \right) \\ &= \frac{1}{2} \log \left( \rho^2 (1 - \rho_1) 2^{-2I(X_1; U_1|Z)} + (1 - \rho_1)(1 - \rho^2) \right) + \frac{1}{2} \log(2\pi e) \\ &\geq \frac{1}{2} \log \left( \rho^2 (1 - \rho_1) 2^{-2R_1} + (1 - \rho_1)(1 - \rho^2) \right) + \frac{1}{2} \log(2\pi e), \end{aligned} \quad (35)$$

where

(34) follows from the entropy power inequality [34] because  $X_1$  and  $B$  are independent given  $(U_1, Z)$ , and

(35) follows because function

$$f(x) = \frac{1}{2} \log(p 2^{-2x} + q)$$

is monotonically decreasing in  $x$  for  $p > 0$ , and we have the rate constraint in (32).

Now (33) and (35) imply

$$\begin{aligned} E &\leq \frac{1}{2} \log \left( \frac{\sigma_{Y|Z}^2}{\rho^2(1 - \rho_1) 2^{-2R_1} + (1 - \rho_1)(1 - \rho^2)} \right) \\ &= \frac{1}{2} \log \left( \frac{1}{1 - \rho^2 + \rho^2 2^{-2R_1}} \right), \end{aligned}$$

which proves that  $(R_1, E)$  is in  $\mathcal{R}_o^G$ . This completes the proof for the region  $\mathcal{D}_1$ .

The proof is analogous for  $(\rho_0, \rho_1)$  in the region  $\mathcal{D}_2$ . The only difference is that under  $H_0$ ,  $X_1$  and  $Y$  can now be expressed as

$$\begin{aligned} X_1 &= \sqrt{\rho_1}Z + \sqrt{\rho_1 - \rho_0}Z' + \sqrt{1 - 2\rho_1 + \rho_0}W \\ Y &= \sqrt{\rho_1}Z - \sqrt{\rho_1 - \rho_0}Z' + \sqrt{1 - 2\rho_1 + \rho_0}V. \end{aligned}$$

Suppose now that  $(\rho_0, \rho_1)$  is in  $\mathcal{D}_3$ . One can verify that  $-\rho_0 - \rho_1 > 0$  here. Hence,  $X_1$  and  $Y$  can be expressed as

$$\begin{aligned} X_1 &= \sqrt{\rho_1}Z + \sqrt{-\rho_0 - \rho_1}Z' + \sqrt{1 + \rho_0}W \\ Y &= -\sqrt{\rho_1}Z - \sqrt{-\rho_0 - \rho_1}Z' + \sqrt{1 + \rho_0}V \end{aligned}$$

under  $H_0$ . Their expressions under  $H_1$  are the same as before. It is evident that  $Z$  is in  $\Xi$ . Therefore, the outer bound in Corollary 7 is valid for this case, which implies that it suffices to show that

$$\tilde{\mathcal{R}}^G \subseteq \mathcal{R}_o^G.$$

Under  $H_0$ , the conditional distribution of  $Y$  given  $Z = z$  is Gaussian with the mean  $-\sqrt{\rho_1}z$  and the variance  $1 - \rho_1$ . Similarly under  $H_1$ , it is Gaussian with the mean  $\sqrt{\rho_1}z$  and the variance  $1 - \rho_1$ . We therefore obtain

$$\begin{aligned} D(p_{Y|Z} \| q_{Y|Z} | Z) &= \int_{z \in \mathbb{R}} p_Z(z) dz \int_{y \in \mathbb{R}} p_{Y|Z}(y|z) \log \frac{p_{Y|Z}(y|z)}{q_{Y|Z}(y|z)} dy \\ &= \int_{z \in \mathbb{R}} p_Z(z) dz \int_{y \in \mathbb{R}} p_{Y|Z}(y|z) \log \left[ \exp \left( \frac{(y - \sqrt{\rho_1}z)^2}{2(1 - \rho_1)} - \frac{(y + \sqrt{\rho_1}z)^2}{2(1 - \rho_1)} \right) \right] dy \\ &= \int_{z \in \mathbb{R}} p_Z(z) dz \int_{y \in \mathbb{R}} p_{Y|Z}(y|z) \left[ -\frac{2(\log e)\sqrt{\rho_1}yz}{1 - \rho_1} \right] dy \\ &= -\frac{2(\log e)\sqrt{\rho_1}}{1 - \rho_1} \int_{z \in \mathbb{R}} zp_Z(z) dz \int_{y \in \mathbb{R}} yp_{Y|Z}(y|z) dy \\ &= -\frac{2(\log e)\sqrt{\rho_1}}{1 - \rho_1} \int_{z \in \mathbb{R}} zp_Z(z) dz (-\sqrt{\rho_1}z) \\ &= \frac{2(\log e)\rho_1}{1 - \rho_1} \int_{z \in \mathbb{R}} z^2 p_Z(z) dz \\ &= \frac{2(\log e)\rho_1}{1 - \rho_1}. \end{aligned}$$

Again, since  $X_1, Y$ , and  $Z$  are jointly Gaussian under  $H_0$ , we can write

$$Y = \rho X_1 - \sqrt{\rho_1}(1 + \rho)Z + B,$$

where  $B$  is defined as before. The rest of the proof is identical to the region  $\mathcal{D}_1$  case.  $\square$

### 8.1.2 Ahlswede and Csiszár's Inner Bound

We next compare the outer bound with Ahlswede and Csiszár's inner bound, which is obtained by using a Gaussian test channel to quantize  $X_1$ . One can use better inner bounds [6, 7], but they are quite complicated and for the Gaussian case considered here, Ahlswede and Csiszár's bound itself is quite close to our outer bound in some cases. Let

$$\mathcal{R}_i^G \triangleq \left\{ (R_1, E) : E \leq \frac{1}{2} \log \left( \frac{1 - \rho_1^2(1 - 2^{-2R_1})}{1 - \rho_0^2(1 - 2^{-2R_1})} \right) - \frac{(\log e)\rho_1(\rho_0 - \rho_1)(1 - 2^{-2R_1})}{1 - \rho_1^2(1 - 2^{-2R_1})} \right\}.$$

**Proposition 2.** [5]  $\mathcal{R}_i^G \subseteq \mathcal{R}^G$ .

*Proof.* Fix any  $(R_1, E)$  in  $\mathcal{R}_i^G$ . Let  $U_1 = X_1 + P$ , where  $P$  is a zero-mean Gaussian random variable independent of  $(X_1, Y)$  such that

$$I(X_1; U_1) = R_1,$$

which implies that the variance of  $P$

$$\sigma_P^2 = \frac{1}{2^{2R_1} - 1}.$$

The covariance matrix of  $(U_1, Y)$  is

$$\mathbf{K}_0 = \begin{bmatrix} 1 + \sigma_P^2 & \rho_0 \\ \rho_0 & 1 \end{bmatrix}$$

under  $H_0$  and is

$$\mathbf{K}_1 = \begin{bmatrix} 1 + \sigma_P^2 & \rho_1 \\ \rho_1 & 1 \end{bmatrix}.$$

under  $H_1$ . It now follows from Ahlswede and Csiszár's scheme [5, Theorem 5] that the achievable exponent is

$$\begin{aligned}
E_{AC} &= D(p_{U_1Y} \| q_{U_1Y}) \\
&= \int_{\mathbf{z} \in \mathbb{R}^2} p_{U_1Y}(\mathbf{z}) \log \frac{p_{U_1Y}(\mathbf{z})}{q_{U_1Y}(\mathbf{z})} d\mathbf{z} \\
&= -\frac{1}{2} \log((2\pi e)^2 \det(\mathbf{K}_0)) - \int_{\mathbf{z} \in \mathbb{R}^2} p_{U_1Y}(\mathbf{z}) \log q_{U_1Y}(\mathbf{z}) d\mathbf{z} \\
&= -\frac{1}{2} \log((2\pi e)^2 \det(\mathbf{K}_0)) - \int_{\mathbf{z} \in \mathbb{R}^2} p_{U_1Y}(\mathbf{z}) \left[ -\frac{(\log e)}{2} \mathbf{z}^T \mathbf{K}_1^{-1} \mathbf{z} - \frac{1}{2} \log((2\pi)^2 \det(\mathbf{K}_1)) \right] d\mathbf{z} \\
&= \frac{1}{2} \log \frac{\det(\mathbf{K}_1)}{\det(\mathbf{K}_0)} - (\log e) + \frac{(\log e)}{2} \int_{\mathbf{z} \in \mathbb{R}^2} p_{U_1Y}(\mathbf{z}) (\mathbf{z}^T \mathbf{K}_1^{-1} \mathbf{z}) d\mathbf{z} \\
&= \frac{1}{2} \log \frac{\det(\mathbf{K}_1)}{\det(\mathbf{K}_0)} - (\log e) + \frac{(\log e)(1 + \sigma_P^2 - \rho_0 \rho_1)}{\det(\mathbf{K}_1)} \\
&= \frac{1}{2} \log \frac{(1 + \sigma_P^2 - \rho_1^2)}{(1 + \sigma_P^2 - \rho_0^2)} - \log e + \frac{(\log e)(1 + \sigma_P^2 - \rho_0 \rho_1)}{(1 + \sigma_P^2 - \rho_1^2)} \\
&= \frac{1}{2} \log \left( \frac{1 - \rho_1^2 (1 - 2^{-2R_1})}{1 - \rho_0^2 (1 - 2^{-2R_1})} \right) - \frac{(\log e) \rho_1 (\rho_0 - \rho_1) (1 - 2^{-2R_1})}{1 - \rho_1^2 (1 - 2^{-2R_1})}.
\end{aligned}$$

This proves that  $(R_1, E)$  is in  $\mathcal{R}^G$ . □

The inner and outer bounds coincide for the test against independence.

**Corollary 8.** (Test against independence, [5, 35]) If  $X_1$  and  $Y$  are independent under  $H_1$ , i.e.,  $\rho_1 = 0$ , then

$$\mathcal{R}^G = \mathcal{R}_o^G = \mathcal{R}_i^G.$$

### 8.1.3 Numerical Results

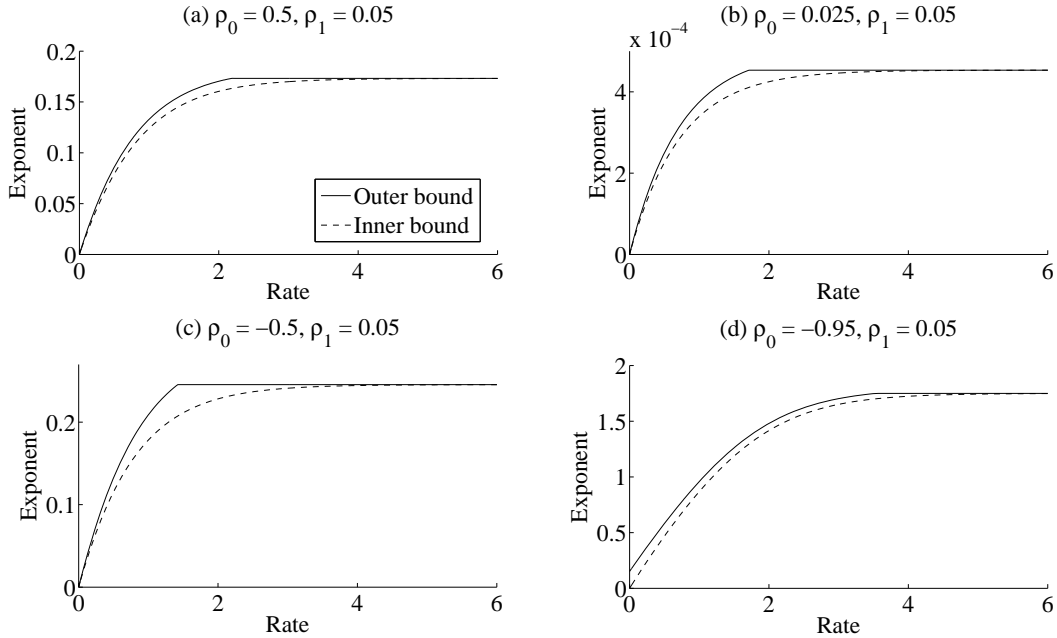


Figure 8: Outer and inner bounds for four examples

Fig. 8 shows the inner and outer bounds for four examples. Fig. 8(a)-(c) are the examples when  $(\rho_0, \rho_1)$  is in  $\mathcal{D}_1 \cup \mathcal{D}_2$ . Observe that the two bounds are quite close near zero and at all large rates. Fig. 8(d) is an example when  $(\rho_0, \rho_1)$  is in  $\mathcal{D}_3$ . For this example, there is a gap between the inner and outer bounds at zero rate. This is due to the fact that in our outer bound, the

joint densities of  $(Y, Z)$  are different under the two hypotheses. Numerical results suggest that for a fixed  $\rho_0$ , the maximum gap between the inner and outer bounds decreases as we decrease  $\rho_1$  and finally becomes zero at  $\rho_1 = 0$ , which is the test against independence.

*Remark 3:* The outer bound can be extended to the vector Gaussian case. One can obtain a single letter outer bound similar to the one in Corollary 7. Then the outer bound can be optimized over all choices of  $U_1$  by using an invertible transformation [36, 37] and the scalar solution obtained above. It follows from our earlier work that the outer bound is tight for the test against independence [38].

## Acknowledgment

This research was supported by the Air Force Office of Scientific Research (AFOSR) under grant FA9550-08-1-0060.

## Appendix A: Proof of Lemma 1

The proof is rather well known and appears in source coding literature quite often. For instance, the similar proof can be found in [16]. Let us define

$$\bar{\Lambda}_i \triangleq \left\{ \lambda_i = (\mathbf{U}, T) \in \Lambda_i : |\mathcal{U}_l| \leq |\mathcal{X}_l| + 2^L - 1 \text{ for all } l \in \mathcal{L}, \text{ and } |\mathcal{T}| \leq 2^L \right\},$$

and

$$\bar{\mathcal{R}}_i^{CI} \triangleq \bigcup_{\lambda_i \in \bar{\Lambda}_i} \mathcal{R}_i^{CI}(\lambda_i).$$

We want to show that  $\mathcal{R}_i^{CI} = \bar{\mathcal{R}}_i^{CI}$ . We start with the deterministic  $T$  case. Consider  $\lambda_i = (\mathbf{U}, T)$  in  $\Lambda_i$ , where  $T$  is deterministic. For any  $S \subseteq \mathcal{L}$  containing 1, we have

$$I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c}, X_{L+1}, Z) = H(\mathbf{X}_S | \mathbf{U}_{S^c}, X_{L+1}, Z) - H(\mathbf{X}_S | \mathbf{U}_{1^c}, U_1, X_{L+1}, Z),$$

and for any nonempty  $S$  not containing 1, we have

$$I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c}, X_{L+1}, Z) = I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c \setminus \{1\}}, U_1, X_{L+1}, Z).$$

Moreover,

$$I(Y; \mathbf{U}, X_{L+1} | Z) = H(Y | X_{L+1}, Z) - H(Y | \mathbf{U}_{1^c}, U_1, X_{L+1}, Z).$$

It follows from the support lemma [32, Lemma 3.4, pp. 310] that there exists  $\bar{U}_1$  with  $\bar{\mathcal{U}}_1 \subseteq \mathcal{U}_1$  such that

$$|\bar{\mathcal{U}}_1| \leq |\mathcal{X}_1| + 2^L - 1,$$

$$\sum_{u_1 \in \bar{\mathcal{U}}_1} \Pr(X_1 = x_1 | U_1 = u_1) \Pr(\bar{U}_1 = u_1) = \Pr(X_1 = x_1) \text{ for all } x_1 \text{ in } \mathcal{X}_1 \text{ but one,}$$

$$H(\mathbf{X}_S | \mathbf{U}_{1^c}, U_1, X_{L+1}, Z) = H(\mathbf{X}_S | \mathbf{U}_{1^c}, \bar{U}_1, X_{L+1}, Z) \text{ for all } S \text{ containing 1,}$$

$$I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c \setminus \{1\}}, U_1, X_{L+1}, Z) = I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c \setminus \{1\}}, \bar{U}_1, X_{L+1}, Z) \text{ for all nonempty } S \text{ not containing 1,}$$

and

$$H(Y | \mathbf{U}_{1^c}, U_1, X_{L+1}, Z) = H(Y | \mathbf{U}_{1^c}, \bar{U}_1, X_{L+1}, Z).$$

Since

$$U_1 \leftrightarrow X_1 \leftrightarrow (\mathbf{U}_{1^c}, \mathbf{X}_{1^c}, X_{L+1}, Y, Z),$$

if we replace  $U_1$  by  $\bar{U}_1$  then the resulting  $\lambda_i$  is in  $\Lambda_i$  and  $\mathcal{R}_i^{CI}(\lambda_i)$  remains unchanged. By repeating this procedure for  $U_2, \dots, U_L$ , we conclude that there exists  $\bar{\lambda}_i = (\bar{\mathbf{U}}, \bar{T})$  in  $\bar{\Lambda}_i$  such that  $\bar{T}$  is deterministic and  $\mathcal{R}_i^{CI}(\lambda_i) = \mathcal{R}_i^{CI}(\bar{\lambda}_i)$ .

We now turn to general  $T$ . Consider  $\lambda_i = (\mathbf{U}, T)$  in  $\Lambda_i$ . Let  $(\mathbf{U}, t)$  denote the joint distribution of  $(\mathbf{U}, T)$  conditioned on  $\{T = t\}$ . It follows from the deterministic  $T$  case that for each  $t$  in  $\mathcal{T}$ , there exists  $\bar{\mathbf{U}}$  such that  $(\bar{\mathbf{U}}, t)$  is in  $\bar{\Lambda}_i$  and  $\mathcal{R}_i^{CI}(\mathbf{U}, t) = \mathcal{R}_i^{CI}(\bar{\mathbf{U}}, t)$ . Hence, on replacing  $\mathbf{U}$  by  $\bar{\mathbf{U}}$  for each  $t$  in  $\mathcal{T}$ , we obtain  $(\bar{\mathbf{U}}, T)$  in  $\bar{\Lambda}_i$  such that  $|\bar{\mathcal{U}}_l| \leq |\mathcal{X}_l| + 2^L - 1$  for all  $l$  in  $\mathcal{L}$  and  $\mathcal{R}_i^{CI}(\mathbf{U}, T) = \mathcal{R}_i^{CI}(\bar{\mathbf{U}}, T)$ . Now  $\mathcal{R}_i^{CI}(\bar{\mathbf{U}}, T)$  is the set of vectors  $(\mathbf{R}, E)$  such that

$$\begin{aligned} \sum_{l \in S} R_l &\geq I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c}, X_{L+1}, Z, T) \text{ for all } S, \text{ and} \\ E &\leq I(Y; \mathbf{U}, X_{L+1} | Z, T). \end{aligned}$$

It again follows from the support lemma that there exists  $\bar{T}$  with  $\bar{\mathcal{T}} \subseteq \mathcal{T}$  such that

$$\begin{aligned} |\bar{\mathcal{T}}| &\leq 2^L, \\ I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c}, X_{L+1}, Z, T) &= I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c}, X_{L+1}, Z, \bar{T}), \text{ and} \\ I(Y; \mathbf{U}, X_{L+1} | Z, T) &= I(Y; \mathbf{U}, X_{L+1} | Z, \bar{T}). \end{aligned}$$

We therefore have that  $\bar{\lambda}_i = (\bar{\mathbf{U}}, \bar{T})$  is in  $\bar{\Lambda}_i$  and  $\mathcal{R}_i^{CI}(\lambda_i) = \bar{\mathcal{R}}_i^{CI}(\bar{\lambda}_i)$ . This proves  $\mathcal{R}_i^{CI} \subseteq \bar{\mathcal{R}}_i^{CI}$ , and hence  $\mathcal{R}_i^{CI} = \bar{\mathcal{R}}_i^{CI}$  because the reverse containment trivially holds.

For part (b), it suffices to show that  $\bar{\mathcal{R}}_i^{CI}$  is closed. Consider any sequence  $(\mathbf{R}^{(n)}, E^{(n)})$  in  $\bar{\mathcal{R}}_i^{CI}$  that converges to  $(\mathbf{R}, E)$ . Since conditional mutual information is a continuous function,  $\bar{\Lambda}_i$  is a compact set. Hence, there exists a sequence  $\lambda_i^{(n)} = (\mathbf{U}^{(n)}, T^{(n)})$  in  $\bar{\Lambda}_i$  that converges to  $\lambda_i = (\mathbf{U}, T)$  in  $\bar{\Lambda}_i$  such that  $(\mathbf{R}^{(n)}, E^{(n)})$  is in  $\bar{\mathcal{R}}_i^{CI}(\lambda_i^{(n)})$ , i.e.,

$$\begin{aligned} \sum_{l \in S} R_l^{(n)} &\geq I(\mathbf{X}_S; \mathbf{U}_S^{(n)} | \mathbf{U}_{S^c}^{(n)}, X_{L+1}, Z, T^{(n)}) \text{ for all } S, \text{ and} \\ E^{(n)} &\leq I(Y; \mathbf{U}^{(n)}, X_{L+1} | Z, T^{(n)}). \end{aligned}$$

Again, by the continuity of conditional mutual information, this implies that

$$\begin{aligned} \sum_{l \in S} R_l &\geq I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c}, X_{L+1}, Z, T) \text{ for all } S, \text{ and} \\ E &\leq I(Y; \mathbf{U}, X_{L+1} | Z, T). \end{aligned}$$

We thus have that  $(\mathbf{R}, E)$  is in  $\bar{\mathcal{R}}_i^{CI}$ .

## Appendix B: Proof of Theorem 1

We prove the deterministic  $T$  case. The general case follows by time sharing. Consider any  $\lambda_i = (\mathbf{U}, T)$  in  $\Lambda_i$  with  $T$  being deterministic. Consider  $(\mathbf{R}, E)$  such that

$$\sum_{l \in S} R_l \geq I(\mathbf{X}_S; \mathbf{U}_S | \mathbf{U}_{S^c}, X_{L+1}, Z) \text{ for all } S \subseteq \mathcal{L}, \text{ and} \quad (36)$$

$$E \leq I(Y; \mathbf{U}, X_{L+1} | Z). \quad (37)$$

It suffices to show that  $(\mathbf{R}, E)$  belongs to the rate-exponent region  $\mathcal{R}_i^{CI}$ .

Consider a sufficiently large block length  $n$ ,  $\epsilon > 0$ , and  $\mu > 0$ . For each  $l$  in  $\mathcal{L}$ , let  $\bar{R}_l = I(X_l; U_l) + \alpha$ , where  $\alpha > 0$ . To construct the codebook of encoder  $l$ , we first generate  $2^{n\bar{R}_l}$  independent codewords  $U_l^n$ , each according to  $\prod_{i=1}^n P_{U_l}(u_{li})$ , and then distribute them uniformly into  $2^{n(R_l+\epsilon)}$  bins. The codebooks and the bin assignments are revealed to the encoders and the detector. The encoding is done in two steps: quantization and binning. The encoder  $l$  first quantizes  $X_l^n$  by selecting a codeword  $U_l^n$  that is jointly  $\mu$ -typical with it. We adopt the typicality notion of Han [6]. If there is more than one such codeword, then the encoder  $l$  selects one of them arbitrarily. If there is no such codeword, it selects an arbitrary codeword. The encoder then sends to the detector the index of the bin to which the codeword  $U_l^n$  belongs. In order to be consistent with our earlier notation, we denote this encoding function by  $f_l^{(n)}$ . It is clear that the rate constraints are satisfied, i.e.,

$$\frac{1}{n} \log |f_l^{(n)}(X_l^n)| = R_l + \epsilon \text{ for all } l \text{ in } \mathcal{L}. \quad (38)$$

The next lemma is a standard achievability result in distributed source coding.

**Lemma 6.** *For any  $\delta > 0, \epsilon > 0, \mu > 0$ , and all sufficiently large  $n$ , there exists a function*

$$\varphi^{(n)} : \prod_{l=1}^L \left\{1, \dots, 2^{n(R_l+\epsilon)}\right\} \times \mathcal{X}_{L+1}^n \times \mathcal{Z}^n \mapsto \prod_{l=1}^L \mathcal{U}_l^n$$

such that (a) if

$$V \triangleq \{\mathbf{U}^n, X_{L+1}^n, Y^n, Z^n \text{ are jointly } \mu\text{-typical under } H_0\},$$

then  $P(V) \geq 1 - \delta$ ; and (b)

$$p_e \triangleq P\left(\varphi^{(n)}\left((f_l^{(n)}(X_l^n))_{l \in \mathcal{L}}, X_{L+1}^n, Z^n\right) \neq \mathbf{U}^n\right) \leq \delta.$$

One can prove this lemma using standard random coding arguments. See [26, 27, 28] for proofs of similar results. Applying this lemma to the hypothesis testing problem at hand, we have

$$\begin{aligned} & \frac{1}{n} I\left(\left(f_l^{(n)}(X_l^n)\right)_{l \in \mathcal{L}}, X_{L+1}^n, Y^n \middle| Z^n\right) \\ &= \frac{1}{n} H(Y^n | Z^n) - \frac{1}{n} H\left(Y^n \middle| \left(f_l^{(n)}(X_l^n)\right)_{l \in \mathcal{L}}, X_{L+1}^n, Z^n\right) \\ &= H(Y|Z) + \frac{1}{n} H\left(\left(f_l^{(n)}(X_l^n)\right)_{l \in \mathcal{L}} \middle| X_{L+1}^n, Z^n\right) - \frac{1}{n} H\left(\left(f_l^{(n)}(X_l^n)\right)_{l \in \mathcal{L}}, Y^n \middle| X_{L+1}^n, Z^n\right). \end{aligned} \quad (39)$$

We can lower bound the second term in (39) as

$$\begin{aligned} \frac{1}{n} H\left(\left(f_l^{(n)}(X_l^n)\right)_{l \in \mathcal{L}} \middle| X_{L+1}^n, Z^n\right) &= \frac{1}{n} I\left(\left(f_l^{(n)}(X_l^n)\right)_{l \in \mathcal{L}}; \mathbf{U}^n \middle| X_{L+1}^n, Z^n\right) \\ &= \frac{1}{n} H(\mathbf{U}^n | X_{L+1}^n, Z^n) - \frac{1}{n} H\left(\mathbf{U}^n \middle| \left(f_l^{(n)}(X_l^n)\right)_{l \in \mathcal{L}}, X_{L+1}^n, Z^n\right) \\ &\geq \frac{1}{n} H(\mathbf{U}^n | X_{L+1}^n, Z^n) - \frac{1}{n} H\left(\mathbf{U}^n \middle| \varphi^{(n)}\left(\left(f_l^{(n)}(X_l^n)\right)_{l \in \mathcal{L}}, X_{L+1}^n, Z^n\right)\right) \end{aligned} \quad (40)$$

$$\geq \frac{1}{n} H(\mathbf{U}^n | X_{L+1}^n, Z^n) - \frac{1}{n} H_b(p_e) - p_e \sum_{l=1}^L \log |\mathcal{U}_l| \quad (41)$$

$$\geq \frac{1}{n} H(\mathbf{U}^n | X_{L+1}^n, Z^n) - \frac{1}{n} - \delta \sum_{l=1}^L \log |\mathcal{U}_l|, \quad (42)$$

where

(40) follows from data processing inequality [34, Theorem 2.8.1],

(41) follows from Fano's inequality [34, Theorem 2.10.1], and

(42) follows Lemma 6(b) and the fact that  $H_b(p_e) \leq 1$ .

The third term in (39) can be upper bounded as

$$\begin{aligned} \frac{1}{n} H \left( \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}}, Y^n \middle| X_{L+1}^n, Z^n \right) &\leq \frac{1}{n} H \left( \mathbf{U}^n, \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}}, Y^n \middle| X_{L+1}^n, Z^n \right) \\ &= \frac{1}{n} H(\mathbf{U}^n, Y^n | X_{L+1}^n, Z^n). \end{aligned} \quad (43)$$

On applying bounds (42) and (43) into (39), we obtain

$$\begin{aligned} &\frac{1}{n} I \left( \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}}, X_{L+1}^n; Y^n \middle| Z^n \right) \\ &\geq H(Y|Z) + \frac{1}{n} H(\mathbf{U}^n | X_{L+1}^n, Z^n) - \frac{1}{n} H(\mathbf{U}^n, Y^n | X_{L+1}^n, Z^n) - \frac{1}{n} - \delta \sum_{l=1}^L \log |\mathcal{U}_l| \\ &= H(Y|Z) - \frac{1}{n} H(Y^n | \mathbf{U}^n, X_{L+1}^n, Z^n) - \frac{1}{n} - \delta \sum_{l=1}^L \log |\mathcal{U}_l| \\ &= H(Y|Z) - \frac{1}{n} H(Y^n, 1_V | \mathbf{U}^n, X_{L+1}^n, Z^n) - \frac{1}{n} - \delta \sum_{l=1}^L \log |\mathcal{U}_l| \\ &= H(Y|Z) - \frac{1}{n} H(1_V | \mathbf{U}^n, X_{L+1}^n, Z^n) - \frac{1}{n} H(Y^n | \mathbf{U}^n, X_{L+1}^n, Z^n, 1_V) - \frac{1}{n} - \delta \sum_{l=1}^L \log |\mathcal{U}_l| \\ &\geq H(Y|Z) - \frac{1}{n} - \frac{1}{n} H(Y^n | \mathbf{U}^n, X_{L+1}^n, Z^n, 1_V = 1) P(V) \\ &\quad - \frac{1}{n} H(Y^n | \mathbf{U}^n, X_{L+1}^n, Z^n, 1_V = 0) P(V^c) - \frac{1}{n} - \delta \sum_{l=1}^L \log |\mathcal{U}_l| \end{aligned} \quad (44)$$

$$\geq H(Y|Z) - \frac{1}{n} H(Y^n | \mathbf{U}^n, X_{L+1}^n, Z^n, 1_V = 1) - \frac{2}{n} - \delta \log |\mathcal{Y}| - \delta \sum_{l=1}^L \log |\mathcal{U}_l|, \quad (45)$$

where

(44) follows from the fact that  $H(1_V | \mathbf{U}^n, X_{L+1}^n, Z^n) \leq 1$ , and

(45) follows from Lemma 6(a) and the facts that

$$\begin{aligned} \frac{1}{n} H(Y^n | \mathbf{U}^n, X_{L+1}^n, Z^n, 1_V = 0) &\leq \log |\mathcal{Y}|, \\ P(V) &\leq 1. \end{aligned}$$

We now proceed to upper bound the second term in (45). Let  $T_\mu^n(\mathbf{U} X_{L+1} Y Z)$  be the set of all jointly  $\mu$ -typical  $(\mathbf{u}^n, x_{L+1}^n, y^n, z^n)$  sequences. We need the following lemma.

**Lemma 7.** [6, Lemma 1(d)] *If  $n$  is sufficiently large, then for any  $(\mathbf{u}^n, x_{L+1}^n, y^n, z^n)$  in  $T_\mu^n(\mathbf{U} X_{L+1} Y Z)$ , we have*

$$P_{Y^n | \mathbf{U}^n, X_{L+1}^n, Z^n}(y^n | \mathbf{u}^n, x_{L+1}^n, z^n) \geq \exp[-n(H(Y | \mathbf{U}, X_{L+1}, Z) + 2\mu)].$$

Using this lemma, we obtain

$$\begin{aligned} \frac{1}{n} H(Y^n | \mathbf{U}^n, X_{L+1}^n, Z^n, 1_V = 1) &= -\frac{1}{n} \sum_{T_\mu^n(\mathbf{U} X_{L+1} Y Z)} P_{\mathbf{U}^n, X_{L+1}^n, Y^n, Z^n | 1_V = 1} \log P_{Y^n | \mathbf{U}^n, X_{L+1}^n, Z^n, 1_V = 1} \\ &= -\frac{1}{n} \sum_{T_\mu^n(\mathbf{U} X_{L+1} Y Z)} P_{\mathbf{U}^n, X_{L+1}^n, Y^n, Z^n | 1_V = 1} \log \frac{P_{Y^n | \mathbf{U}^n, X_{L+1}^n, Z^n}}{P_{1_V = 1 | \mathbf{U}^n, X_{L+1}^n, Z^n}} \\ &\leq \sum_{T_\mu^n(\mathbf{U} X_{L+1} Y Z)} P_{\mathbf{U}^n, X_{L+1}^n, Y^n, Z^n | 1_V = 1} (H(Y | \mathbf{U}, X_{L+1}, Z) + 2\mu) \\ &= H(Y | \mathbf{U}, X_{L+1}, Z) + 2\mu. \end{aligned} \quad (46)$$

Substituting (46) into (45) gives

$$\begin{aligned} \frac{1}{n} I \left( \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}}, X_{L+1}^n; Y^n \middle| Z^n \right) &\geq I(Y; \mathbf{U}, X_{L+1}|Z) - \frac{2}{n} - 2\mu - \delta \log |\mathcal{Y}| - \delta \sum_{l=1}^L \log |\mathcal{U}_l| \\ &\geq E - 3\mu - \delta \log |\mathcal{Y}| - \delta \sum_{l=1}^L \log |\mathcal{U}_l|, \end{aligned} \quad (47)$$

where the last inequality follows from (37) and the fact that  $n$  can be made arbitrarily large. We conclude from (38) and (47) that

$$\left( R_1 + \epsilon, \dots, R_L + \epsilon, E - 3\mu - \delta \log |\mathcal{Y}| - \delta \sum_{l=1}^L \log |\mathcal{U}_l| \right)$$

is in  $\mathcal{R}_*^{CI}$ . Since this is true for any  $\delta > 0, \epsilon > 0$ , and  $\mu > 0$ , we have that  $(\mathbf{R}, E)$  is in  $\overline{\mathcal{R}_*^{CI}}$ . This together with Corollary 1 implies that  $(\mathbf{R}, E)$  is in  $\mathcal{R}^{CI}$ .

## Appendix C: Proof of Theorem 2

Suppose  $(\mathbf{R}, E)$  is in  $\mathcal{R}_*^{CI}$ . Then there exists a block length  $n$  and encoders  $f_l^{(n)}$  such that

$$R_l \geq \frac{1}{n} \log \left| f_l^{(n)}(X_l^n) \right| \text{ for all } l \text{ in } \mathcal{L}, \text{ and} \quad (48)$$

$$E \leq \frac{1}{n} I \left( \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}}, X_{L+1}^n; Y^n \middle| Z^n \right). \quad (49)$$

Consider any  $X$  in  $\chi$ . Let  $T$  be a time sharing random variable uniformly distributed over  $\{1, \dots, n\}$  and independent of  $(\mathbf{X}^n, X_{L+1}^n, X^n, Y^n, Z^n)$ . Define

$$\begin{aligned} X_l &= X_l^n(T) \text{ for each } l \text{ in } \mathcal{L} \cup \{L+1\}, \\ X &= X^n(T), \\ Y &= Y^n(T), \\ Z &= Z^n(T), \\ U_l &= \left( f_l^{(n)}(X_l^n), X^n(1:T-1), X_{L+1}^n(T^c), Z^n(T^c) \right) \text{ for each } l \text{ in } \mathcal{L}, \text{ and} \\ W &= (X^n(T^c), X_{L+1}^n(T^c), Z^n(T^c)). \end{aligned}$$

It is easy to verify that  $\lambda_o = (\mathbf{U}, W, T)$  is in  $\Lambda_o$  and

$$X \leftrightarrow (\mathbf{X}, X_{L+1}, Y, Z) \leftrightarrow \lambda_o.$$

It suffices to show that  $(\mathbf{R}, E)$  is in  $\mathcal{R}_o^{CL}(X, \lambda_o)$ . We obtain the following from (49)

$$\begin{aligned}
E &\leq \frac{1}{n} I \left( \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}}, X_{L+1}^n; Y^n \middle| Z^n \right) \\
&= \frac{1}{n} \left[ H(Y^n | Z^n) - H \left( Y^n \middle| \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}}, X_{L+1}^n, Z^n \right) \right] \\
&= \frac{1}{n} \sum_{i=1}^n \left[ H(Y^n(i) | Z^n(i)) - H \left( Y^n(i) \middle| \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}}, Y^n(1:i-1), X_{L+1}^n, Z^n \right) \right] \\
&\leq \frac{1}{n} \sum_{i=1}^n \left[ H(Y^n(i) | Z^n(i)) - H \left( Y^n(i) \middle| \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}}, Y^n(1:i-1), X^n(1:i-1), X_{L+1}^n, Z^n \right) \right] \quad (50)
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{n} \sum_{i=1}^n \left[ H(Y^n(i) | Z^n(i)) - H \left( Y^n(i) \middle| \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}}, X^n(1:i-1), X_{L+1}^n, Z^n \right) \right] \quad (51) \\
&= \frac{1}{n} \sum_{i=1}^n I \left( Y^n(i); \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}}, X^n(1:i-1), X_{L+1}^n(i^c), Z^n(i^c), X_{L+1}^n(i) \middle| Z^n(i) \right) \\
&= I(Y^n(T); \mathbf{U}, X_{L+1}^n(T) | Z^n(T), T) \\
&= I(Y; \mathbf{U}, X_{L+1} | Z, T),
\end{aligned}$$

where

(50) follows from conditioning reduces entropy, and

(51) follows because of the Markov chain

$$Y^n(1:i-1) \leftrightarrow (X^n(1:i-1), Z^n(1:i-1)) \leftrightarrow \left( \left( f_l^{(n)}(X_l^n) \right)_{l \in \mathcal{L}}, X_{L+1}^n, Y^n(i), Z^n(i:n) \right).$$

Now let  $S \subseteq \mathcal{L}$ . Then (48) implies

$$\begin{aligned}
n \sum_{l \in S} R_l &\geq \sum_{l \in S} \log \left| f_l^{(n)}(X_l^n) \right| \\
&\geq \sum_{l \in S} H \left( f_l^{(n)}(X_l^n) \right) \\
&\geq H \left( \left( f_l^{(n)}(X_l^n) \right)_{l \in S} \right) \\
&\geq H \left( \left( f_l^{(n)}(X_l^n) \right)_{l \in S} \middle| \left( f_l^{(n)}(X_l^n) \right)_{l \in S^c}, X_{L+1}^n, Z^n \right) \quad (52)
\end{aligned}$$

$$\begin{aligned}
&= I \left( X^n, \mathbf{X}_S^n; \left( f_l^{(n)}(X_l^n) \right)_{l \in S} \middle| \left( f_l^{(n)}(X_l^n) \right)_{l \in S^c}, X_{L+1}^n, Z^n \right) \\
&= I \left( X^n; \left( f_l^{(n)}(X_l^n) \right)_{l \in S} \middle| \left( f_l^{(n)}(X_l^n) \right)_{l \in S^c}, X_{L+1}^n, Z^n \right) \\
&\quad + I \left( \mathbf{X}_S^n; \left( f_l^{(n)}(X_l^n) \right)_{l \in S} \middle| \left( f_l^{(n)}(X_l^n) \right)_{l \in S^c}, X^n, X_{L+1}^n, Z^n \right) \\
&= \sum_{i=1}^n I \left( X^n(i); \left( f_l^{(n)}(X_l^n) \right)_{l \in S} \middle| \left( f_l^{(n)}(X_l^n) \right)_{l \in S^c}, X^n(1:i-1), X_{L+1}^n, Z^n \right) \\
&\quad + \sum_{l \in S} I \left( X_l^n; f_l^{(n)}(X_l^n) \middle| X^n, X_{L+1}^n, Z^n \right), \quad (53)
\end{aligned}$$

where

(52) follows from conditioning reduces entropy, and

(53) follows because  $X$  is in  $\chi$ .

We next lower bound the second sum in (53).

$$\begin{aligned}
& I\left(X_l^n; f_l^{(n)}(X_l^n) \middle| X^n, X_{L+1}^n, Z^n\right) \\
&= \sum_{i=1}^n I\left(X_l^n(i); f_l^{(n)}(X_l^n) \middle| X^n, X_l^n(1:i-1), X_{L+1}^n, Z^n\right) \\
&= \sum_{i=1}^n \left[ H\left(X_l^n(i) \middle| X^n, X_l^n(1:i-1), X_{L+1}^n, Z^n\right) - H\left(X_l^n(i) \middle| f_l^{(n)}(X_l^n), X^n, X_l^n(1:i-1), X_{L+1}^n, Z^n\right) \right] \\
&\geq \sum_{i=1}^n \left[ H\left(X_l^n(i) \middle| X^n, X_{L+1}^n, Z^n\right) - H\left(X_l^n(i) \middle| f_l^{(n)}(X_l^n), X^n, X_{L+1}^n, Z^n\right) \right] \tag{54} \\
&= \sum_{i=1}^n I\left(X_l^n(i); f_l^{(n)}(X_l^n) \middle| X^n, X_{L+1}^n, Z^n\right), \tag{55}
\end{aligned}$$

where (54) again follows from conditioning reduces entropy. On applying (55) in (53), we obtain

$$\begin{aligned}
\sum_{l \in S} R_l &\geq \frac{1}{n} \sum_{i=1}^n \left[ I\left(X^n(i); \left(f_l^{(n)}(X_l^n)\right)_{l \in S} \middle| \left(f_l^{(n)}(X_l^n)\right)_{l \in S^c}, X^n(1:i-1), X_{L+1}^n, Z^n\right) \right. \\
&\quad \left. + \sum_{l \in S} I\left(X_l^n(i); f_l^{(n)}(X_l^n) \middle| X^n, X_{L+1}^n, Z^n\right) \right]. \tag{56}
\end{aligned}$$

If  $S^c$  is nonempty, then continuing from (56) gives

$$\begin{aligned}
\sum_{l \in S} R_l &\geq I\left(X^n(T); \mathbf{U}_S \middle| \mathbf{U}_{S^c}, X_{L+1}^n(T), Z^n(T), T\right) \\
&\quad + \sum_{l \in S} I\left(X_l^n(T); U_l \middle| X^n(T), X_{L+1}^n(T), Z^n(T), X^n(T^c), X_{L+1}^n(T^c), Z^n(T^c), T\right) \\
&= I\left(X; \mathbf{U}_S \middle| \mathbf{U}_{S^c}, X_{L+1}, Z, T\right) + \sum_{l \in S} I\left(X_l; U_l \middle| X, W, X_{L+1}, Z, T\right).
\end{aligned}$$

Finally if  $S = \mathcal{L}$ , then

$$\begin{aligned}
& I\left(X^n(i); \left(f_l^{(n)}(X_l^n)\right)_{l \in S} \middle| \left(f_l^{(n)}(X_l^n)\right)_{l \in S^c}, X^n(1:i-1), X_{L+1}^n, Z^n\right) \\
&= I\left(X^n(i); \left(f_l^{(n)}(X_l^n)\right)_{l \in S} \middle| X^n(1:i-1), X_{L+1}^n, Z^n\right) \\
&= I\left(X^n(i); \left(f_l^{(n)}(X_l^n)\right)_{l \in S}, X^n(1:i-1), X_{L+1}^n(i^c), Z^n(i^c) \middle| X_{L+1}^n(i), Z^n(i)\right). \tag{57}
\end{aligned}$$

Substituting (57) into (56) yields

$$\sum_{l \in \mathcal{L}} R_l \geq I\left(X; \mathbf{U} \middle| X_{L+1}, Z, T\right) + \sum_{l \in \mathcal{L}} I\left(X_l; U_l \middle| X, W, X_{L+1}, Z, T\right).$$

This completes the proof of Theorem 2.

## Appendix D: Proof of Lemma 2

It suffices to show that (C6) implies (C7). The other direction immediately follows by letting  $\epsilon \rightarrow 0$ . We can assume without loss of generality that  $|\mathcal{X}| \geq 2$  because the lemma trivially holds otherwise. Let  $\mathcal{X} = \{1, 2, \dots, |\mathcal{X}|\}$  be the alphabet set of  $X$ . Let  $P_i$  be the  $i$ th row of the stochastic matrix  $P_{Y|X}$  corresponding to  $X = i$ . We need the following lemma.

**Lemma 8.** *If (C6) holds, then rows  $P_i$  corresponding to positive  $P_X(i)$  are distinct.*

*Proof.* The proof is by contradiction. Suppose that  $P_X(1)$  and  $P_X(2)$  are positive and  $P_1 = P_2$ . Let us define a random variable  $U$  as

$$U \triangleq \begin{cases} 2 & \text{if } X = 1, 2 \\ X & \text{otherwise.} \end{cases}$$

The stochastic matrix  $P_{X|U}$  has

$$\begin{aligned} P_{X|U}(1|2) &= \frac{P_X(1)}{P_X(1) + P_X(2)}, \\ P_{X|U}(2|2) &= \frac{P_X(2)}{P_X(1) + P_X(2)}, \text{ and} \\ P_{X|U}(i|i) &= 1 \text{ for all } i \text{ in } \{3, 4, \dots, |\mathcal{X}|\}. \end{aligned}$$

It is easy to see that  $Y, X$ , and  $U$  form a Markov chain

$$Y \leftrightarrow X \leftrightarrow U. \quad (58)$$

We now have

$$\begin{aligned} H(Y|U) &= \sum_{i=2}^{|\mathcal{X}|} H(Y|U=i)P_U(i) \\ &= H(Y|U=2)P_U(2) + \sum_{i=3}^{|\mathcal{X}|} H(Y|U=i)P_U(i) \\ &= H\left(\sum_{j=1}^{|\mathcal{X}|} P_j P_{X|U}(j|2)\right) P_U(2) + \sum_{i=3}^{|\mathcal{X}|} H\left(\sum_{j=1}^{|\mathcal{X}|} P_j P_{X|U}(j|i)\right) P_U(i) \\ &= H(P_2) P_U(2) + \sum_{i=3}^{|\mathcal{X}|} H(P_i) P_U(i) \\ &= \sum_{i=2}^{|\mathcal{X}|} H(P_i) P_U(i), \end{aligned} \quad (59)$$

and

$$\begin{aligned} H(Y|X) &= \sum_{j=1}^{|\mathcal{X}|} H(P_j) P_X(j) \\ &= \sum_{j=1}^{|\mathcal{X}|} H(P_j) \left( \sum_{i=2}^{|\mathcal{X}|} P_{X|U}(j|i) P_U(i) \right) \\ &= \sum_{i=2}^{|\mathcal{X}|} P_U(i) \sum_{j=1}^{|\mathcal{X}|} P_{X|U}(j|i) H(P_j) \\ &= P_U(2) \sum_{j=1}^{|\mathcal{X}|} P_{X|U}(j|2) H(P_j) + \sum_{i=3}^{|\mathcal{X}|} P_U(i) \sum_{j=1}^{|\mathcal{X}|} P_{X|U}(j|i) H(P_j) \\ &= P_U(2) H(P_2) + \sum_{i=3}^{|\mathcal{X}|} P_U(i) H(P_i) \\ &= \sum_{i=2}^{|\mathcal{X}|} P_U(i) H(P_i). \end{aligned} \quad (60)$$

Now (58) through (60) together imply that  $I(X; Y|U) = 0$ , and hence  $Y \leftrightarrow U \leftrightarrow X$ . However,

$$\begin{aligned} H(X|U) &= \sum_{i=2}^{|\mathcal{X}|} H(X|U=i)P_U(i) \\ &= H(X|U=2)P_U(2) \\ &= H_b\left(\frac{P_X(1)}{P_X(1) + P_X(2)}\right) (P_X(1) + P_X(2)) \\ &> 0, \end{aligned}$$

which contradicts our assumption that (C6) holds. □

Consider any  $U$  that satisfies the Markov chain

$$U \leftrightarrow X \leftrightarrow Y.$$

We can assume without loss of generality that  $P_U(u)$  is positive for all  $u$  in  $\mathcal{U}$  because only positive  $P_U(u)$  contributes to  $H(X|U)$  and  $I(X; Y|U)$  in conditions (C6) and (C7). Then

$$\begin{aligned} I(X; Y|U) &= H(Y|U) - H(Y|X) \\ &= \sum_{u \in \mathcal{U}} H(Y|U=u) P_U(u) - \sum_{i=1}^{|\mathcal{X}|} P_X(i) H(P_i) \\ &= \sum_{u \in \mathcal{U}} H \left( \sum_{i=1}^{|\mathcal{X}|} P_i P_{X|U}(i|u) \right) P_U(u) - \sum_{i=1}^{|\mathcal{X}|} \left( \sum_{u \in \mathcal{U}} P_{X|U}(i|u) P_U(u) \right) H(P_i) \\ &= \sum_{u \in \mathcal{U}} P_U(u) \left[ H \left( \sum_{i=1}^{|\mathcal{X}|} P_i P_{X|U}(i|u) \right) - \sum_{i=1}^{|\mathcal{X}|} P_{X|U}(i|u) H(P_i) \right] \\ &= \sum_{u \in \mathcal{U}} P_U(u) T(P_{X|U}(\cdot|u)), \end{aligned} \tag{61}$$

where (61) follows by setting

$$T(P_{X|U}(\cdot|u)) \triangleq H \left( \sum_{i=1}^{|\mathcal{X}|} P_i P_{X|U}(i|u) \right) - \sum_{i=1}^{|\mathcal{X}|} P_{X|U}(i|u) H(P_i).$$

Since entropy is a strictly concave and continuous function,  $T$  is a nonnegative continuous function of  $P_{X|U}(\cdot|u)$ . Moreover, for any  $u$  in  $\mathcal{U}$ ,  $P_{X|U}(i|u) = 0$  for all  $i$  in  $\mathcal{X}$  such that  $P_X(i) = 0$ . Let  $\mathcal{P}$  denote the set of all such  $P_{X|U}(\cdot|u)$ . Define

$$\gamma(\delta) \triangleq \sup_{P \in \mathcal{P}} \{H(P) : T(P) \leq \delta\}.$$

It now follows from Lemma 8 that if  $T(P) = 0$  for some  $P$  in  $\mathcal{P}$ , then  $P$  must be a point mass and hence  $H(P) = 0$ . Therefore,  $\gamma(0) = 0$ . We next show that  $\gamma$  is continuous at 0. Consider a nonnegative sequence  $\delta_n \rightarrow 0$ . Then there exists a sequence of distributions  $P_n$  in  $\mathcal{P}$  such that

$$T(P_n) \leq \delta_n \tag{62}$$

$$H(P_n) \geq \frac{\gamma(\delta_n)}{2}. \tag{63}$$

Now, since the set of all distributions on  $\mathcal{X}$  is a compact set, by considering a subsequence, we can assume without loss of generality that  $P_n$  converges to  $P$  in  $\mathcal{P}$ . By letting  $n \rightarrow \infty$  in (62), we obtain that  $T(P) = 0$ , i.e.,  $P$  is a point mass. Therefore,  $H(P) = 0$ . It now follows from (63) that  $\gamma(\delta_n) \rightarrow 0 = \gamma(0)$  as  $n \rightarrow \infty$ . Hence,  $\gamma$  is continuous at 0.

Fix  $0 < \epsilon < \log |\mathcal{X}|$  (condition (C7) is always true for  $\epsilon \geq \log |\mathcal{X}|$ ). Choose  $\epsilon_1 > 0$  such that  $\gamma(\epsilon_1/\log |\mathcal{X}|) + \epsilon_1 = \epsilon$ . Set  $\delta = (\epsilon_1/\log |\mathcal{X}|)^2$ . Let  $I(X; Y|U) \leq \delta$ . Define the sets

$$\mathcal{U}_1 \triangleq \{u \in \mathcal{U} : T(u) \leq \sqrt{\delta}\} \text{ and } \mathcal{U}_2 \triangleq \mathcal{U} \setminus \mathcal{U}_1.$$

Note that  $\mathcal{U}_1$  is nonempty because  $\delta < 1$ . We now have

$$\begin{aligned} \delta &\geq I(X; Y|U) \\ &= \sum_{u \in \mathcal{U}} P_U(u) T(u) \\ &\geq \sum_{u \in \mathcal{U}_2} P_U(u) T(u) \\ &> \sqrt{\delta} \sum_{u \in \mathcal{U}_2} P_U(u), \end{aligned}$$

which implies

$$\sum_{u_2} P_U(u) < \sqrt{\delta}.$$

Hence,

$$\begin{aligned} H(X|U) &= \sum_{u_1} H(X|U = u)P_U(u) + \sum_{u_2} H(X|U = u)P_U(u) \\ &< \gamma(\sqrt{\delta}) + \sqrt{\delta} \log |\mathcal{X}| \\ &= \gamma(\epsilon_1/\log |\mathcal{X}|) + \epsilon_1 \\ &= \epsilon. \end{aligned}$$

## References

- [1] T. He and L. Tong, “Detection of information flows,” *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 4925-4945, Nov. 2008.
- [2] A. Agaskar, T. He, and L. Tong, “Distributed detection of multi-hop information flows with fusion capacity constraints,” *IEEE Trans. Sig. Proc.*, vol. 58, no. 6, pp. 3373-3383, June 2010.
- [3] T. Berger, “Decentralized estimation and decision theory,” in *IEEE 7th Spring Workshop on Inf. Theory*, Mt. Kisco, NY, Sept. 1979.
- [4] T. S. Han and S. Amari, “Statistical inference under multiterminal data compression,” *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2300-2324, Oct. 1998.
- [5] R. Ahlswede and I. Csiszár, “Hypothesis testing with communication constraints,” *IEEE Trans. Inf. Theory*, vol. 32, no. 4, pp. 533-542, July 1986.
- [6] T. S. Han, “Hypothesis testing with multiterminal data compression,” *IEEE Trans. Inf. Theory*, vol. 33, no. 6, pp. 759-772, Nov. 1987.
- [7] H. Shimokawa, T. S. Han, and S. Amari, “Error bound of hypothesis testing with data compression,” in *IEEE Int. Symp. Inf. Theor. Proc.*, 1994, p. 29.
- [8] D. Slepian and J. K. Wolf, “Noiseless coding of correlated information sources,” *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471-480, July 1973.
- [9] B. G. Kelly and A. B. Wagner, “Reliability in source coding with side information,” preprint.
- [10] B. G. Kelly, A. B. Wagner, and A. Vamvatsikos, “Error exponents and test channel optimization for the Gaussian Wyner-Ziv problem,” in *IEEE Int. Symp. Inf. Theor. Proc.*, 2008, pp. 414-418.
- [11] B. G. Kelly and A. B. Wagner, “Error exponents and test channel optimization for the Wyner-Ziv problem,” in *Proc. 45th Annual Allerton Conference*, 2007.
- [12] Y. Kochman and G. W. Wornell, “On the excess distortion exponent of the quadratic-Gaussian Wyner-Ziv problem,” in *IEEE Int. Symp. Inf. Theor. Proc.*, 2010, p. 36-40.
- [13] I. Csiszár, “Linear codes for sources and source networks: error exponents, universal coding,” *IEEE Trans. Inf. Theory*, vol. 28, no. 4, pp. 585-592, July 1982.

- [14] B. G. Kelly and A. B. Wagner, "Improved source coding exponents via Witsenhausen's rate," preprint.
- [15] I. Csiszár and J. Körner, "Graph decomposition: a new key to coding theorems," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 5-12, Jan. 1981.
- [16] A. B. Wagner and V. Anantharam, "An improved outer bound for multiterminal source coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1919-1937, May 2008.
- [17] S. Tavildar, P. Viswanath, and A. B. Wagner, "The Gaussian many-help-one distributed source coding problem," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 564-581, Jan. 2010.
- [18] A. B. Wagner, S. Tavildar, and P. Viswanath, "Rate region of the quadratic Gaussian two-encoder source-coding problem," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1938-1961, May 2008.
- [19] A. B. Wagner, "On distributed compression of linear functions," in *Proc. 46th Annual Allerton Conference*, 2008, pp. 1546-1553.
- [20] Ozarow, "On a source-coding problem with two channels and three receivers," *Bell Sys. Tech. J.*, vol. 59, no. 10, pp. 1909-1921, 1980.
- [21] H. Wang and P. Viswanath, "Vector Gaussian multiple description with two levels of receivers," *IEEE Trans. Inf. Theory*, vol. 55, no. 1, pp. 401-410, Jan. 2009.
- [22] S. I. Gel'fand and M. S. Pinsker, "Coding of sources on the basis of observations with incomplete information," (in Russian), *Problemy Peredachi Informatsii*, vol. 15, no. 2, pp. 45-57, April-June 1979.
- [23] Y. Oohama, "Rate-distortion theory for Gaussian multiterminal source coding systems with several side informations at the decoder," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2577-2593, July 2005.
- [24] V. Prabhakaran, D. Tse, and K. Ramchandran, "Rate region of the quadratic Gaussian CEO problem," in *IEEE Int. Symp. Inf. Theor. Proc.*, 2004, p. 117.
- [25] C. Tian and J. Chen, "Successive refinement for hypothesis testing and lossless one-helper problem," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4666-4681, Oct. 2008.
- [26] T. Berger, "Multiterminal source coding," in *The Information Theory Approach to Communications*, ser. CISM Courses and Lectures, G. Longo, Ed. Springer-Verlag, 1978, vol. 229, pp. 171-231.
- [27] S. Y. Tung, "Multiterminal source coding," Ph.D. dissertation, School of Electrical Engineering, Cornell University, Ithaca, NY, May 1978.
- [28] M. Gastpar, "The Wyner-Ziv problem with multiple sources," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2762-2768, Nov. 2004.
- [29] J. Chen, X. Zhang, T. Berger, and S. B. Wicker, "An upper bound on the sum-rate distortion function and its corresponding rate allocation schemes for the CEO problem," *IEEE J. Select. Areas Commun.*, vol. 22, no. 6, pp. 977-987, Aug. 2004.
- [30] P. Viswanath, "Sum rate of a class of Gaussian multiterminal source coding problems," in *Advances in Network Information Theory*, ser. DIMACS in Discrete Mathematics and Theoretical Computer Science, P. Gupta, G. Kramer, and A. J. van Wijngaarden, Eds. AMS, 2004, vol. 66, pp. 43-60.

- [31] A. B. Wagner, B. G. Kelly, and Y. Altuğ, “The lossy one-helper conjecture is false,” in *Proc. 47th Annual Allerton Conference*, 2009, pp. 716-723.
- [32] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 1st ed. Academic, New York, 1981.
- [33] J. Wang, J. Chen, and X. Wu, “On the minimum sum rate of Gaussian multiterminal source coding: new proofs,” in *IEEE Int. Symp. Inf. Theor. Proc.*, 2009, pp. 1463-1467.
- [34] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York: John Wiley & Sons, 2005.
- [35] Y. Oohama, “Gaussian multiterminal source coding,” *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1912-1923, Nov. 1997.
- [36] C. Tian and J. Chen, “Remote vector Gaussian source coding with decoder side information under mutual information and distortion constraints,” *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4676-4680, Oct. 2009.
- [37] A. Globerson and N. Tishby, “On the optimality of the Gaussian information bottleneck curve,” in *Hebrew Univ. Tech. Report*, 2004.
- [38] Md. S. Rahman and A. B. Wagner, “Vector Gaussian hypothesis testing and lossy one-helper problem,” in *IEEE Int. Symp. Inf. Theor. Proc.*, 2009, pp. 968-972.